UNIVERSIDADE FEDERAL DE SANTA CATARINA
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

Glauco Vinicius Scheffel

Segurança na Avaliação de Conhecimento em Contexto não Presencial

Dissertação submetida à Universidade Federal de Santa Catarina como parte dos requisitos para a obtenção do grau de Mestre em Ciência da Computação.

Florianópolis, Agosto de 2002

Segurança na Avaliação de Conhecimento em Contexto não Presencial

Glauco Vinicius Scheffel

Esta Dissertação foi julgada adequada para a obtenção do título de Mestre em Ciência da Computação Sistemas de Computação e aprovada em sua forma final pelo Programa de Pós-Graduação em Ciência da Computação.

Prof. Dr. Fernando Ostuni Gauthier

Banca Examinadora

Prof. Dr. Alejandro Martins

Prof. Dr. Clovis Torres Fernandes

Prof. Dr. Ricardo Felipe Custódio

Ofereço esta dissertação à minha esposa, Clara Carolina Seixa e aos meus pais, Maria Aracy Foss Scheffel e Nei Roberto Scheffel, que me ajudaram a continuar neste caminho.

Agradecimentos

Este trabalho não foi escrito isoladamente, ele seria impossível sem a ajuda do professor Ricardo Felipe Custódio que me apresentou a idéia geral do problema e as ferramentas básicas que deram fundamentação à proposta feita neste trabalho. Foram de grande valor a ajuda da minha esposa durante os meus constantes tropeços com o LaTeX. Agradeço ainda a pessoas que contribuíram diretamente com opiniões ou artigos como Ubirajara Maia de Oliveira e Augusto Jun Devigili. A estes muito obrigado e minha eterna dívida.

Sumário

Lista de Figuras

Lista de Tabelas

Lista de Siglas

AC	Autoridade de Certificação
AD	Autoridade de Datação
$PDDE$	Protocoladora digital de documentos eletrônicos
C	Texto cifrado
CD	Certificado Digital
DC	Processo inverso de EC, decifrar
DP	Processo inverso de EP, decifrar
EC	Cifrar usando criptografia simétrica
EP	Cifrar usando criptografia asimétrica
H	Função resumo (*hash*)
K_S	Chave de sessão
KR_i	Chave Privada de i
KU_i	Chave Pública de i
LCR	Lista de certificados revogados
$LDAP$	Diretório público
RP	Rede de Petri
M	Texto aberto, ou seja, não cifrado
S	Assinar
V	Verificar a assinatura, retorna um valor lógico indicando a autenticidade
X	Texto Aberto - texto de forma que pode ser entendido
Y	Texto Cifrado - texto de forma que não é possível entender

Resumo

Realizou-se um estudo sobre o uso da Internet para aplicação de avaliações de conhecimento onde os alunos encontram-se afastados das instituições e não são supervisionados por pessoas no momento da avaliação. O estudo é adequado aos seguintes tipos de avaliação: cursos a distância, certificação profissional, proficiência em idiomas e concursos públicos. O estudo focou-se em determinar a aplicabilidade do uso desta como canal para transmissão e aplicação de avaliações sob o ponto de vista dos problemas de segurança do canal e autenticidade dos documentos. Demonstra-se a importância da etapa de avaliação dentro do processo de ensino a distância; enumeram-se o funcionamento e os problemas de segurança que se pode encontrar nos vários tipos de avaliação existentes; faz-se uma revisão de soluções encontradas na literatura; resumem-se conceitos de criptografia e, por último, propõe-se uma nova arquitetura que permita o uso da Internet como meio seguro de realização de avaliações.

Abstract

It was made a study about the Internet use for application of knowledge evaluation where students are out of the institution and are not supervised in the moment of the evaluation. The study is adequated to the following kind of evaluations: course of distance learning, professional certification, language proficiency and public contests. The study was focused in determine the applicability of the use of the Internet as a mean of transmission and application of evaluation under the security problem viewpoint, this work gives attention to the channel security and documents authenticity. It demonstrates the importance of the phase of evaluation in the distance teaching process; it enumerates the admission process and security problems that can be found in various kinds of evaluations already available; it reviews the solutions encountered in the literature; it summarizes cryptography concepts and, also, it proposes a new architecture that makes the Internet a secure mean of evaluation administrator.

Capítulo 1

Introdução

Popularizado o acesso a Internet, surgem novas formas de comunicação, interação e troca de conhecimentos, as quais não consideram as distâncias físicas e temporais. Este modelo de comunicação pode ser usado para criar uma nova sala de aula onde, de acordo com Tarouco [TAR 00], o seguinte pode ser visualizado:

> ”A integração da educação e tecnologias interativas possibilita atividades educacionais assíncronas, sem a exigência de presenças físicas e simultâneas de professor e alunos, transformando a sala de aula em um espaço *virtual* ”

Mesmo com a distância possível por causa desse espaço ”virtual”, cabe ainda ao professor acompanhar o desempenho dos alunos através do uso de avaliações. Ou seja, este deve emitir juízo de valor e para tanto medir e comparar os desempenhos [dMdM 97]. A figura 1.1 mostra uma ilustração deste espaço. Avaliações de conhecimento existem também em vestibulares, concursos e certificações profissionais. O desenvolvimento de avaliações válidas realizadas em larga escala através de computadores no novo espaço requer mais pesquisas. Partindo desta premissa, o Laboratório de Segurança em Computação (LabSEC), do Curso de Pós-graduação em Computação, da Universidade Federal de Santa Catarina, vem desenvolvendo uma série de trabalhos que adotam técnicas de criptografia, com o objetivo de fornecer mecanismos de segurança para serviços que usam a Internet como canal de transmissão. Esta dissertação é parte integrante dos estudos realizados no LabSEC para implementação de protocolos criptográficos que permitam a realização de

avaliações seguras a distância através da Internet, procurando preencher lacunas relacionadas a segurança do processo de avaliação, detalhes sobre estas lacunas podem ser encontrado na Justificativa do trabalho 1.2.

Este capítulo apresenta uma visão geral de como e porque esta dissertação foi escrita. Inicia-se com os objetivos e motivos que levaram a escolha do tema e justifica a importância deste. Ao final é fornecida uma idéia geral dos materiais e métodos adotados e da estrutura do trabalho.

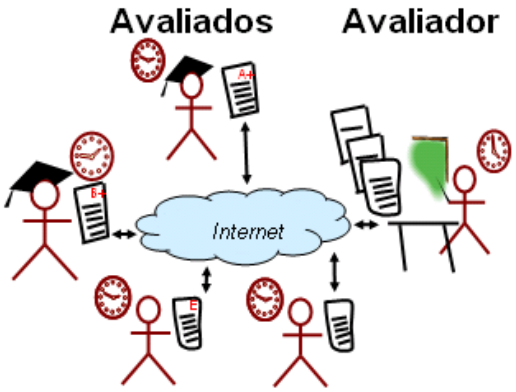

Figura 1.1: Avaliador e Avaliados estão separados no espaço. O avaliador representado na extrema direita da figura, interage com os avaliados que podem estar: na rede da instituição que esta realizando a avaliação, em uma rede privada qualquer com acesso a internet, ou podem estar acessando a Internet de casa.

1.1 Objetivos

1.1.1 Objetivo Geral

Propor um protocolo criptográfico que possa usar tecnologias de redes de computadores para fornecer segurança e validade jurídica aos documentos da avaliação de conhecimento realizada a distância. Como resultado, tornar possível a realização de avaliações onde avaliador e avaliados encontrem-se separados no espaço, fornecendo assim meios para discussão, aperfeiçoamento e, algum dia, regulamentação desse processo.

1.1.2 Objetivos Específicos

- Determinar os principais locais onde avaliações são aplicadas;
- Definir as atividades que fazem parte do processo de avaliação;
- Apresentar a importância das avaliações;
- Encontrar e descrever as fases que compõem o processo de avaliação;
- Definir que documentos são necessários durante as fases que compõem o processo de avaliação;
- Verificar, quando necessário, as questões relacionadas com a legislação do processo de avaliação;
- Estabelecer as vulnerabilidades que poderiam advir da transformação do processo tradicional em um processo de avaliação não presencial a distância;
- Revisar as tecnologias que podem ser usadas para fornecer segurança em comunicação digital;
- Revisar as tecnologias que podem ser usadas para garantir a autenticidade e integridade de documentos eletrônicos;
- Propor um protocolo para avaliação a distância que incorpore tecnologias que garantam a integridade e autenticidade dos documentos;
- Formalizar o protocolo proposto.

1.1.3 Convenções e Definições

Por uma questão de simplificação, optou-se por agrupar os tipos de avaliação, descritos no Capítulo 2, nos seguintes modelos:

- **Competição**: Testes onde se determina através da atribuição de notas quem possui maior conhecimento em uma área. Útil, por exemplo, em concursos públicos ou vestibulares.

- **Avaliação do conhecimento**: Testes que medem o desenvolvimento de um aluno em curso, que pode ser virtual ou presencial. Testes onde se precisa determinar o grau de conhecimento de alguém em uma área específica, tal como certificação profissional ou proficiência em idiomas.

1.2 Justificativa

Muito cuidado deve-se ter com o uso de mecanismos que automatizem o processo de avaliação do conhecimento. A tarefa de fornecer e garantir a validade destas avaliações é extremamente complexa, já que estão envolvidos diversos sub-processos que, em geral, são simples quando executados de forma tradicional. Estão presentes diversas circunstâncias elementares que determinam a validade da avaliação em cursos, concursos e vestibulares. O avaliador espera que a avaliação seja executada de forma que os avaliados demonstrem seu real conhecimento. A ausência destas circunstâncias torna o processo inútil. Para evitar que isto ocorra, o avaliador deve garantir o seguinte:

- Os avaliados não acessem as questões da avaliação antes da data e hora marcados;
- Os avaliados não acessem o resultado antes da data e hora marcados;
- Um avaliado não responda as questões em uma data e hora diferentes do estabelecido para a realização da avaliação;
- As respostas não sejam alteradas após a avaliação ter sido entregue;
- As respostas sejam atribuídas a outro avaliado durante ou após a avaliação;
- Os avaliados não ”colem”; ou seja, dois ou mais avaliados troquem informações sobre respostas para as questões da avaliação, ou os avaliados usem uma anotação, livro ou ferramenta, como uma calculadora, de forma oculta e sem permissão no decorrer da avaliação, para obter a resposta correta das questões;
- Um avaliado não seja substituído por uma pessoa com grandes conhecimentos na área, no momento da avaliação, praticando falsidade ideológica; ou seja, uma pes-

soa utilize-se de documentos falsificados ou alterados e finja ser o avaliado e realize a avaliação no lugar deste.

Os dois últimos itens da lista anterior não fazem parte do objetivo desta dissertação, mas são tratados no trabalho de [FIO 00], o qual ressalta o fato de que a segurança em um sistema comercial tem o cliente agindo na maior parte dos casos como aliado. Como exemplo, em um sistema bancário normalmente não há interesse do cliente em divulgar sua senha ou permitir de alguma forma que estranhos tenham pleno acesso e controle sobre sua conta corrente. Fiorese [FIO 00] vê o avaliado como um inimigo em potencial onde, ”a *personificação* do usuário pode vir a ocorrer com conivência, isto é, o avaliado pede para outra pessoa fazer a avaliação em seu lugar. Deste modo, são necessários métodos que procurem minimizar este problema ou, pelo menos, dificultar este procedimento. Sabe-se, porém, que por mais sofisticada que seja a solução, sempre poderão existir métodos para enganar o sistema”. Esta visão pode facilmente ser aplicada para concursos e vestibulares. O trabalho de Fiorese é analisado na Seção 4.3.

O avaliado espera e acredita que a avaliação seja justa, de forma que o seguinte ocorra, conforme o tipo de avaliação:

- **Avaliação do conhecimento**- Ele receba a nota correta, ou seja, a nota é atribuída de acordo com seu desempenho.
- **Competição**- Ele e os demais avaliados tenham condições iguais, de acordo com o seguinte:
  - Apenas avaliados inscritos de forma regular, na atividade de inscrição, possam participar da atividade de avaliação;
  - Ninguém poderá realizar a avaliação fora da data e hora marcadas para a atividade de avaliação;
  - As avaliações não tenham sido lidas por nenhum avaliado após a atividade de inscrição e antes da atividade de aplicação;
  - As respostas não tenham sido lidas por nenhum avaliado após a atividade de inscrição e antes da atividade de aplicação;

- as avaliações contenham as mesmas questões para todos os avaliados durante a atividade de avaliação;
- as avaliações sejam corrigidas da mesma forma na atividade de apuração;
- nenhum avaliado responda as questões em uma data e hora diferentes da estabelecida para a atividade de avaliação;
- as respostas dadas pelo avaliado não possam ser alteradas após a atividade de avaliação ter sido finalizada.

Os processo que compõem a avaliação do conhecimento são representados usando diagramas de atividade ou de casos de uso pertencentes a *Unified Modeling Language* (*UML*) [JAC 95, JAC 98, PJ 01, QUA 98]. A UML foi adotada por ser um padrão de fato e um padrão de mercado que esta disponível em diversas ferramentas de modelagem de sistemas.

1.3 Motivação

A Internet recentemente emergiu como uma solução que mudou radicalmente como as empresas fazem negócios, sendo que muitos processos vêm sendo transferidos para esta. Os processos relacionados com o ensino, normalmente, realizam as avaliações de forma presencial, obrigando os avaliados a deslocar-se de sua residência ou trabalho em datas e horários predeterminados para um local onde serão supervisionados durante o processo. A realização presencial é necessária devido à falta de mecanismos que ofereçam, por exemplo, valor legal à avaliação realizada a distância. Avaliador e avaliados precisam de um conjunto de garantias para que possam aceitar a transferência desse processo. Ressalte-se que o chamado *comércio eletrônico* é uma realidade hoje em dia, mesmo sem a aplicação de técnicas que garantam todo o processo de compra e venda. Neste trabalho estudam-se os aspectos relacionados à segurança e são definidos requisitos para permitir que a avaliação a distância seja feita de forma tão segura quanto a avaliação presencial, ou melhor. Os requisitos por sua vez são a matéria-prima adotada para criação de um protocolo que seja capaz de garantir segurança do canal e autenticidade dos docu-

mentos. Do protocolo definido espera-se que ocorra sua aplicação e ajuste, em avaliações de pequena escala, com a transferência de avaliações de certificações profissionais e de avaliações de cursos a distância. No futuro, talvez distante, espera-se que o protocolo depurado pelo tempo e pelo uso seja útil em avaliações mais complexas, como, por exemplo, vestibulares.

1.4 Trabalhos Relacionados

Fiorese [FIO 00] descreve uma alternativa para avaliação segura do conhecimento a distância, detalhado na seção 4.3, focando no controle necessário durante a atividade de aplicação. Tarouco [TAR 00] possui diversos trabalhos na área de ensino a distância com uso de redes de computadores e diversos de seus artigos foram úteis para entendimento do tópico ensino a distância. A empresa Prometric fornece um produto de extrema qualidade para realização de avaliações presenciais, com centros de testes localizados em diversos países, incluindo capitais de estados da federação Brasileira. O trabalho deles é detalhado na subseção 2.4.2.

1.5 Materiais e Métodos

A *Unified Modeling Language* (*UML*) [JAC 95, JAC 98, PJ 01, QUA 98] foi usada para modelar as atividades do processo de avaliação. Os diagramas foram desenhados na ferramenta *Rational Rose*, que pode ser encontrada no endereço da Rational na Internet: *http://www.rational.com/tryit/evals/roseeval.jsp*. Algumas etapas do protocolo foram validadas em um protótipo que foi desenvolvido usando a linguagem Java. As ferramentas de desenvolvimento para Java podem ser encontradas no endereço *http://java.sun.com/downloads.html*. O protótipo serviu apenas como forma de validar teorias e não é tratado neste trabalho. As mensagens trocadas entre as máquinas cliente e servidor estão no formato *XML*, que tem sua especificação disponível no endereço *http://www.w3c.org/XML/*.

1.6 Requisitos de Segurança na Avaliação a Distância

De forma geral, conforme [FIL 01], uma avaliação possui como atividades o seguinte: convocação e divulgação, inscrição, preparação, aplicação, apuração, classificação, publicação e revisão. Estas são executadas conforme o modelo apresentado no diagrama de *Diagrama de atividades* da Figura 1.2. Um processo de avaliação inicia com a atividade de convocação que define as regras para a realização do processo. Após o final do processo de convocação as atividades de inscrição e preparação são executadas em paralelo. Quando finalizadas as duas atividades, o processo é executado de forma seqüencial. Mais detalhes são apresentados posteriormente na subseção 2.2.4.

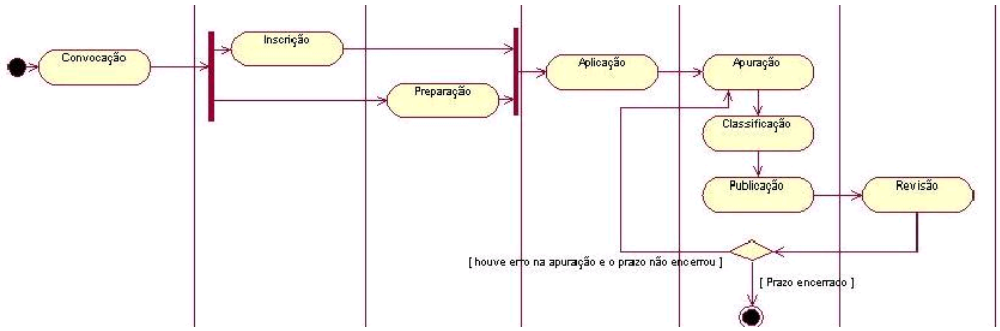

Figura 1.2: Linha de tempo para avaliações do conhecimento

Em cada uma das atividades existem requisitos diferentes relacionados com a segurança. Para guiar o desenvolvimento deste trabalho, tais requisitos estão listados abaixo:

- **Convocação e divulgação** - A instituição, ao disponibilizar e divulgar a convocação em meio eletrônico, espera que o documento não seja passível de adulteração;
- **Inscrição** - A instituição espera que nenhum nome seja inserido na lista de inscritos de forma ilícita, ou seja, sem pagar as taxas ou fora do período de inscrição. O candidato, por sua vez, espera que ninguém consiga se inscrever fora do período permitido;
- **Avaliação** - Na Seção 1.2 estão descritos princípios que guiam esta etapa, em torno da qual as demais orbitam;

- **Apuração** - Os mesmos critérios de correção devem ser adotados para todos os candidatos;
- **Classificação** - As notas devem ser ordenadas corretamente de acordo com o desempenho de cada avaliado que foi atribuído;
- **Publicação** - As notas publicadas devem corresponder às que foram atribuídas na atividade de apuração;
- **Revisão** - Todo e qualquer candidato tem o direito de solicitar revisão do gabarito adotado para apuração. O candidato que solicita a revisão tem direito de receber retorno sobre sua solicitação;
- **Divulgação** - O resultado de qualquer solicitação de revisão que gere alteração no resultado da apuração deve ser amplamente divulgado para todos avaliados;

1.7 Organização do Texto

Este trabalho basicamente está agrupado em três tópicos. Primeiro ele provê uma revisão sobre o processo de avaliação do conhecimento de forma tradicional, apresentando sua aplicabilidade e importância. Essa revisão é útil para aqueles que desejam entender de maneira clara o contexto no qual este trabalho está inserido. Esta primeira parte está dividida da seguinte maneira: O Capítulo 2 apresenta uma relação de tipos de avaliação encontrados, no momento da criação deste trabalho de pesquisa, e descreve o funcionamento e características destes tipos. No capítulo 2 analisam-se diversos tipos de avaliação e seus ambientes distintos e como as avaliações são aplicadas atualmente nestes ambientes. No Capítulo 3 mostra-se a avaliação como uma das etapas do ensino a distância e como as avaliações vêm sendo aplicadas e os efeitos do modelo atual. No Capítulo 4 mostram-se sistemas e proposta de sistemas de avaliação que são aplicados a distância.

O segundo grupo foca nas tecnologias que servem de base para a construção de um modelo computacional do processo que foi anteriormente revisado, onde o

texto no Capítulo 5 revisa os conceitos relacionados ao uso da criptografia como forma de obter segurança em meio computacional. Por último faz-se a proposta do protocolo no Capítulo 6 revisando e detalhando o processo de avaliação e propondo um cenário informatizado, finaliza-se o trabalho no Capítulo 7 com a formalização e validação do protocolo proposto.

Capítulo 2

Aplicação de Avaliações

2.1 Introdução

O primeiro passo, na criação de um protocolo que forneça validade jurídica e segurança dos documentos usados na avaliação do conhecimento tendo a *internet* como meio de transmissão, é a determinação de onde as avaliações são usadas. O segundo é a definição de como é executado o processo de avaliação. O primeiro passo é dado com a listagem abaixo:

- **Competição** - usadas no seguinte:
  - **Concursos públicos**: avaliações realizadas com o objetivo de selecionar o melhor candidato para um cargo público;
  - **Concursos vestibulares**: avaliações realizadas com o objetivo de selecionar o melhor candidato para uma vaga em uma instituição de ensino superior;
- **Avaliação do conhecimento** - usadas no seguinte:
  - **Cursos** avaliações são executadas ao longo de todo o processo com objetivo de permitir ao avaliador medir o aprendizado e fornecer ao avaliado um visão sobre seu aproveitamento. Os cursos podem ser a distância ou presenciais;
  - **Certificação profissional**: avaliações servem para comprovar o conhecimento de um produto, tecnologia, técnica ou conceito;

– **Proficiência em idiomas**: avaliações usadas para determinar as habilidades em um idioma tal como, por exemplo, o *Test of English as a Foreign Language* (*TOEFL*);

Apesar de aplicadas em ambientes distintos todas possuem o objetivo de mensurar o conhecimento de um avaliado. Para mensurar, diversas técnicas podem ser usadas [dMdM 97], a saber :

- Exercício de avaliação baseado em problemas;
- Testes de múltipla escolha, onde uma entre várias opções está correta;
- Avaliação através de prova escrita;
- Prova prática;
- Avaliação da performance em atividades práticas;
- Avaliação de habilidades;
- Avaliação comportamental;
- Avaliação em trabalhos;
- Avaliação em testes orais.

O mais comum é que se aplique nas *competições* a avaliação *objetiva* também conhecida como avaliação de *múltipla escolha*, na qual deve-se marcar a(s) alternativa(s) correta(s). O sistema convencional para provas de múltipla escolha consiste de atribuir uma pontuação para cada resposta correta. Pode-se adotar o sistema de correção com penalização onde, de acordo com [FIL 01], nas questões de múltipla escolha pode-se cancelar uma resposta certa para cada resposta errada. Avaliação através de prova escrita, na forma de redação, são obrigatórias para testes de seleção para ingresso no terceiro grau, por força de lei desde dezembro de 2001.

Fala-se neste capítulo sobre como as avaliações são aplicadas atualmente, com o objetivo de analisar o funcionamento destas e entender como cada uma

pode influenciar a avaliação não presencial a distância quando forem implementados em um sistema computacional. As duas primeiras seções apresentam o uso de avaliações em *competições*, conforme definido na subsecção 1.1.3, explicando o processo usado na seção 2.2 (*concursos públicos*) e na seção 2.3 (*vestibulares*). As demais, por sua vez, apresentam o processo adotado em *avaliações do conhecimento*, conforme modelo definido na subseção 1.1.3. Aqui este modelo foi representado por 2.4 (*certificações*) e 2.5 *(avaliação em sala de aula*).

2.2 Concurso Público

O concurso público encontra-se definido pela lei $8112/90$ como a única forma de nomeação para cargo de carreira ou cargo isolado em órgãos públicos [dMFD 01]. Acima de tudo um concurso público é um sistema de escolha baseado no mérito, pois fornece a certeza de que todos podem participar e permite que os melhores candidatos realmente sejam escolhidos [FIL 01].

2.2.1 Princípios

A existência dos concursos públicos é justificada pelos princípios da igualdade e impessoalidade, legalidade, publicidade, moralidade e da probidade da coisa pública [dMFD 01]. Ressalta-se que qualquer processo administrativo só pode ser considerado válido se estiver de acordo com estes princípios [FIL 01]. Estes princípios são definidos no Capítulo VII do Título III e no artigo 37 da constituição vigente. Os princípios são detalhados a seguir:

- **Princípio da legalidade** - Qualquer atividade administrativa deve ser autorizada por lei, ou seja, o estado deve respeitar as próprias leis que edita. Neste caso tem-se a lei $8112/90$;

- **Princípio da igualdade e impessoalidade** - Impessoal é ”o que não pertence a uma pessoa em especial”. Ou seja, aquilo que não pode ser voltado especialmente a

determinadas pessoas, tratando a todos de forma idêntica. De acordo com [FIL 01] ”Este princípio tem proteção no direito positivo: o artigo segundo, alínea e, da Lei número $47171/65$ que regula a ação popular, culmina com a sanção de invalidade o desvio de finalidade”;

- **Princípio da moralidade** - Onde o administrador público deve sempre distinguir o que é honesto do que é desonesto;

- **Princípio da publicidade** - Impõe que atos administrativos devam merecer a mais ampla divulgação possível, pois propiciam a possibilidade de controlar a legitimidade e a transparência dos atos administrativos Lesivo;

- **Probidade** - Causador de dano efetivo ou presumido ao patrimônio público.

A inobservância das normas de que trata o concurso público implica em nulidade do ato e a punição da autoridade responsável [dMFD 01].

2.2.2 Equipe

Não foram encontradas na legislação ou na bibliografia consultada referências a equipe necessária para realização de um concurso público, por esta razão recomenda-se aqui a adoção de um modelo semelhante ao apresentado para concursos vestibulares como apresentado em 2.3.2.

2.2.3 Infra-estrutura

Existem diversas Universidades e entidades sem fins lucrativos que realizam a preparação e o controle logístico de concursos públicos, a existência destas não implica em impedimento do orgão público que irá realizar o concurso controlar e gerir todo o processo. Uma visão mais detalhada sobre a estrutura física necessária pode ser encontrada a seguir em 2.3.3.

2.2.4 Atividades

O processo de avaliação inicia com a definição por parte da autoridade nomeada para coordenar o processo, do seguinte:

- Banca elaboradora;
- Banca corretora;
- Regras para realização do processo de avaliação.

Depois de definidas as regras de convocação, estas devem ser publicadas em um edital de convocação. A atividade de inscrição é iniciada dentro do prazo definido pelo edital e enquanto candidatos se inscrevem a banca elaboradora pode paralelamente preparar as avaliações. Finalizadas as inscrições e a preparação, cabe aos avaliados aguardar o início da atividade de avaliação, que deve ser na data e hora definidas no edital. A atividade de distribuição tem que ser iniciada em tempo, antes do início da avaliação, para que exista:

- Uma cópia da avaliação para cada um dos candidatos;
- Um gabarito para cada candidato colocar suas respostas;
- Um ambiente que servirá como local de avaliação;
- Um fiscal por ambiente, como responsabilidade de monitorar o processo de avaliação;
- Uma ata na qual cada um dos candidatos pode colocar sua assinatura como comprovante de seu comparecimento;

O responsável pela atividade de distribuição deve definir quantos ambientes serão necessários para realização da avaliação. A quantidade de locais de avaliação é determinada pela relação entre o espaço disponível em cada local e a quantidade de avaliados que estão inscritos. No momento da distribuição normalmente procura-se manter uma distribuição semi-simétrica de avaliados por local de avaliação, por exemplo, existindo 2 ambientes de 40 lugares e um total de 65 inscritos para uma avaliação pode-se dividir os avaliados em um grupo de 32 e o restante em um grupo de 33. Na data e hora definidas os

candidatos comparecem ao local de avaliação, e após responder as avaliações e seguir as normas definidas para o processo devem aguardar a publicação do seu aproveitamento. A data e os veículos de comunicação que serão usados para publicação devem ser definidos no edital de convocação. A publicação do resultado ocorre após a banca corretora analisar e atribuir valor para cada uma das avaliações. Terminada a atribuição inicia-se a atividade de classificação na qual o resultado obtido pelos candidatos é ordenado de forma que seja simples demonstrar quem foram os melhores candidatos. Resumidamente, o processo aqui descrito é composto, conforme definido por [FIL 01], pelas seguintes atividades:

- Convocação e divulgação;
- Inscrição;
- Preparação;
- Avaliação;
- Apuração;
- Classificação;
- Publicação;
- Revisão;
- Divulgação.

A lista apresentada não corresponde completamente à proposta definida por [FIL 01], pois foi acrescentado o item *Preparação*. Cada uma das atividades acima listadas são detalhadas logo a seguir.

2.2.5 Convocação e Divulgação

A validade e condições de realização do concurso público devem estar adstritas ao edital de convocação, que comandará todo o processo seletivo [dMFD 01]. Um edital de convocação para concurso público deve conter, de acordo com sugestão de [dMFD 01], o seguinte:

1. Indicação - Número e data do edital
2. Objeto do Edital - Onde são detalhados quais cargos serão preenchidos pelo edital
3. Dos cargos - Onde os cargos são descritos minuciosamente com informações como as seguintes:
    - Denominação do cargo;
    - Escolaridade mínima;
    - Habilitação legal;
    - Retribuição;
    - Jornada de trabalho;
    - Lotação;
    - Atribuições do cargo;
    - Número de vagas.
4. Requisitos para posse - Onde devem constar informações que podem restringir acesso ao cargo, tais como as seguintes:
    - Nacionalidade;
    - Idade mínima;
    - Estar em dia com obrigações militares, se homem;
    - Estar em dia com obrigações eleitorais;
    - Apresentar declaração de capacidade física e mental para exercício do cargo;
    - Apresentar declaração de bens que constituem seu patrimônio;
    - Declaração de que não acumula cargo, emprego ou função pública.
5. Das inscrições - Onde deve constar as seguintes informações:
    - Local;
    - Período;

- Se a inscrição pode ser feita por procuração ou não;
- Reserva de vagas para portadores de deficiência física de no mínimo 20

6. Da realização - Onde deve constar o seguinte:
    - Local;
    - Cronograma das suas etapas;
    - Hora de comparecimento para ingresso no recinto;
    - Hora para início da avaliação;
    - Forma de ingresso;
    - Condições de realização da prova quanto a consulta bibliográfica, uso de máquinas e instrumentos em geral;
7. Do Programa - Onde deve constar o seguinte:
    - Indicação das disciplinas;
    - Discriminação dos conteúdos que serão abordados;
    - Especificação da bibliografia básica adotada;
8. Do processo seletivo - Onde o seguinte especificado:
    - Discriminação das etapas;
    - Procedimentos de avaliação, tais como notas mínimas e peso das questões;
9. Correção de provas - Onde o seguinte deve constar:
    - Indicação dos métodos de correção para questões objetivas, de múltipla escolha e subjetivas;
10. Da classificação e dos recursos - De acordo com o seguinte;
    - Critérios para classificação;
    - Critérios de desempate;

- Afixação de gabaritos para fins de recursos, se for o caso;
- Forma de apresentação de recursos;
- Vista de prova pelos candidatos;
- Procedimentos que devem ser seguidos para solicitar revisão;
- Instância para julgamento de recursos;

11. Outras disposições - Onde o seguinte deve ser definido:

- Validade do concurso, que não pode ser superior a dois anos;
- Indicação expressa de que a inscrição do candidato implica conhecimento e aceite de todos os termos do edital;

A divulgação da convocação pelo *diário oficial da união*, ou *DOU*, por no mínimo três dias é obrigatória. O concurso deve ser realizado no prazo mínimo de 45 dias, a contar da primeira publicação no *DOU* na forma do \$ $4o$ do art 22 da lei número $8666/9312$ Taxa de inscrição e o valor deve ser fixado no edital, quando indispensável o seu custeio, ressalvadas as hipóteses de isenção nele expressamente previstas (Redação dada ao artigo 11 da lei número $8112/90$ e nas de número 9527 e $10.12.97$). A Figura 2.1 resume o processo de convocação e divulgação

2.2.6 Preparação

Não foram encontradas referências que expliquem como devem ser elaboradas as questões que irão compor as avaliações nos concursos, por esta razão recomenda-se que seja adotado um processo semelhante ao encontrado para concursos vestibular, descrito em 2.3.6.

2.2.7 Inscrição

Esta etapa é a manifestação da vontade do candidato em participar do concurso [FIL 01] bem como seu contrato de aceite das regras que definem o edital.

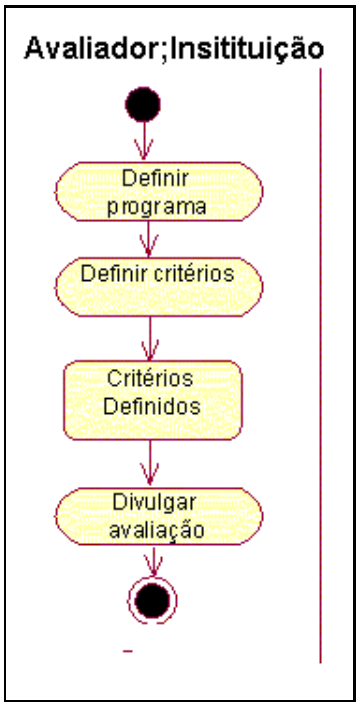

Figura 2.1: Seqüência do processo de convocação e divulgação. Uma convocação é tipicamente um processo sequencial onde deve-se: definir o programa, definir critérios e divulgar a avaliação. O diagrama também demonstra que antes da divulgação apenas a instituição, normalmente representada por um presidente, e uma pessoa de confiança deste, denominada avaliador, devem ter acesso ao edital de convocação.

2.2.8 Aplicação

O candidato deve comparecer ao local designado para a realização da prova (*local de prova*), com antecedência mínima definida pelo edital, munido dos itens especificados no edital como, por exemplo, caneta esferográfica azul ou preta e portando os documentos de identificação requisitados tais como: carteira de identidade e cartão de identificação. Garante-se acesso ao candidato que estiver sido previamente inscrito e apresentar o original de um documento de identificação, como, por exemplo um dos seguintes: a) Cédula Oficial de Identidade; b) Carteira expedida por Órgão ou Conselho de Classe com valor de documento de identidade (Lei 6.206, 07 de maio de 1975); ou c) Carteira Nacional de Habilitação (modelo novo, com foto). Observa-se que não

se aceitam cópias, mesmo que sejam autenticadas, e o documento de identificação deverá estar em perfeitas condições, de forma a permitir, com clareza, a identificação do candidato e deverá conter, obrigatoriamente, fotografia recente. A identificação é realizada pelo *fiscal*, sendo que é comum durante este processo de identificação solicitar que o candidato assine uma ata a qual pode ser usada para comprovação futura da presença. Durante a realização das provas normalmente não se admite qualquer espécie de consulta ou comunicação entre os candidatos ou destes com outras pessoas. Costuma-se ainda não permitir o uso de equipamentos receptores de mensagens, telefones celulares, ou qualquer equipamento mecânico ou eletrônico que possa operar resultados. Os candidatos têm ainda, por obrigação, permanecer no local da prova por um tempo mínimo como, por exemplo, dois terços do tempo total destinado à realização da prova. O candidato é automaticamente desclassificado se for constatado um ou mais dos seguintes itens:

- utilizar-se ou tentar utilizar-se de meios ilícitos para a resolução da prova;
- contrariar determinações do Fiscal ou cometer qualquer ato de indisciplina durante a realização das provas;
- faltar a qualquer das provas ou chegar ao Local de Prova após o horário previsto, ainda que por motivo de força maior;
- fornecer indícios para identificação da documentação distribuída, tais como assinatura fora do local apropriado, sinal ou indicação óbvia.

O fiscal não pode ficar sozinho com nenhum dos avaliados durante o período que a avaliação estiver sendo executada, devendo permanecer com ele no mínimo três avaliados. Para evitar dúvidas sugere-se que, as regras adotadas sejam definidas no edital do concurso.

2.2.9 Apuração

Provas de título adotadas em alguns concursos públicos não possuem poder de aprovação ou reprovação, só podem refletir-se na classificação dos candidatos

garantindo assim o princípio da impessoalidade inscrito no artigo 37 da Constituição Federal. Como não foram encontradas referências que definissem regras a serem adotadas durante a atividade de apuração nos concursos sugere-se o uso das mesmas técnicas dos concurso vestibular, apresentado na subseção 2.3.9.

2.2.10 Classificação

O critério adotado para determinar os classificados e o peso das diversas formas deve ser publicado no Edital de convocação. Cabe ainda ao edital determinar os critérios que serão adotados para desempate.

2.2.11 Publicação

Deve-se definir em edital como será feita a divulgação.

2.2.12 Revisão

Caso algum candidato julgue que houve erro no gabarito publicado ele deve solicitar revisão do item que considera errado. Se da análise dos pedidos de revisão dos itens das provas resultar anulação de algum deles, o ponto correspondente ao item anulado será atribuído a todos os candidatos que realizaram a prova [FIL 01]. Sugere-se que o Edital defina quanto tempo após a publicação o candidato tem para encaminhar seu pedido de revisão.

2.3 Concurso Vestibular

De acordo com o [eC 01]:

> ”Atualmente são oferecidas 635 mil vagas para ingresso no Ensino Superior. Concorreram a elas $2,8$ milhões de inscritos por ano, o que corresponde a uma relação média de quatro alunos por vaga. ”

Não estando democratizado ainda o acesso ao ensino superior a lei de número 9.394, de 1996 conhecida como *Lei de Diretrizes e Bases da Educação (LDB)* define no seu artigo 44 que o acesso à graduação se dará somente àqueles que, depois de concluído o ensino médio ou equivalente, se candidatarem e se classificarem em processo seletivo. Como se pode observar, algum tipo de processo seletivo deve ser adotado pelas instituições, e neste processo a avaliação de uma redação escrita pelo candidato é obrigatória conforme portaria 2.941 de dezembro de 2001. Esta seção tratará apenas do processo seletivo conhecido como vestibular.

2.3.1 Princípios

Com a demanda por vagas superior a oferta mecanismos de seleção se justificam pelo princípio da igualdade e impessoalidade.

2.3.2 Equipe

A equipe necessária é definida por [CON 02] como sendo formada pelo seguinte:

1. Convocação

   Presidente - Responsável por coordenar e supervisionar o trabalho de todas as equipes. Cabe ao presidente dar início ao processo ao definir em conjunto com uma outra pessoa, aqui denominado avaliador, dar início ao processo de avaliação definindo as regras do edital;

2. Preparação

   Banca elaboradora - Aqueles que são reponsáveis por elaborar a avaliação;

   Elaborador - Aquele que é responsável por elaborar uma avaliação, sendo membro da *banca elaboradora*;

   Informática - Aqueles que são responsáveis por digitar e guardar de forma segura as questões;

3. Distribuição

Informática - Aqueles que ficam responsáveis por imprimir os originais que serão usados para gerar as avaliações;

Apoio Aqueles que estão encarregados da entrega e da preparação do local ou locais onde serão realizadas as avaliações. Fazem parte deste grupo: seguranças, motoristas, faxineiras;

4. Aplicação

Apoio - Grupo responsável por auxiliar os fiscais;

Coordenador de aplicação - Responsável por coordenar e treinar os *fiscais*;

Fiscais - Grupo dos responsáveis por supervisionar o processo de aplicação;

Fiscal - Aquele que é responsável por supervisionar o processo a avaliação, sendo membro do *grupo de fiscais*;

5. Correção

Banca corretora - grupo formado pelos responsáveis pela atribuição de valor às avaliações;

Corretor - Aquele que atribui valor a uma avaliação após analisada, sendo membro da *banca corretora*;

Fiscais de correção - Grupo formado pelas pessoas responsáveis por garantir o cumprimento das normas durante a correção;

Fiscal de correção - Aquele que supervisiona o processo de correção, sendo membro do grupo de *fiscais de correção*;

Informática - Aqueles que estão responsáveis por digitalizar as respostas para as perguntas de *múltipla escolha* e executar os programas que atribuem valor a estas respostas;

6. Publicação

Informática - Aqueles que estão responsáveis por emitir a relação de classificados;

2.3.3 Infra-estrutura

Diversas Universidades, públicas e privadas, possuem uma comissão permanente de vestibular responsável por gerir o processo de seleção de candidatos e promover uma discussão do que realmente se pretende avaliar, auxiliando a executar as avaliações de acordo com as expectativas da instituição e do candidato. Existem comissões permanentes responsáveis pelo processo de seleção de instituições que possuem grande quantidade de candidatos ou uma grande quantidade de cursos cita-se, por exemplo, Unicamp [ACA 02] que em 2002 teve 47.265 candidatos inscritos para seus 50 cursos. Supondo que cada local de avaliação (*sala*), usado pela Unicamp, possua 40 lugares tem-se um total de 1182 salas usadas para realizar a avaliação dos candidatos. Havendo em cada sala um fiscal e um auxiliar de fiscal, conforme afirmado pela Unicamp, descobre-se que houveram aproximadamente 2364 pessoas trabalhando no processo de fiscalização. Outros valores e mais detalhes podem ser obtidos no livro que está disponível na página da Unicamp na *Internet*. A grandeza dos números permitir perceber que um processo bem definido e documentado é o mínimo necessário para coordenar um vestibular, pois existe neste problemas de escala, como grande número de avaliados, um curto espaço de tempo entre atividades e requisitos rígidos no que se refere a segurança e transparência da execução. Cabe à comissão definir e executar e monitorar o processo. Como a Unicamp não é a única instituição a adotar esse modelo, lista-se, a título de exemplo, a seguir as seguintes comissões permanentes:

- **CONVEST**, comissão permanente para os vestibulares da UNICAMP, que pode ser encontrada no endereço eletrônico em *http://www.convest.unicamp.br/*;
- **Fundação CESGRANRIO**, instituída por dez universidades públicas e particulares, encontrada no endereço eletrônico *http://www.cesgranrio.org.br/*;
- **Coperve**, comissão permanente para os vestibulares da UFSC, que pode ser encontrada em *http://www.coperve.ufsc.br/*;

Uma lista completa das comissões permanentes para as Universidades Federais e seu respectivo endereço na Internet pode ser encontrada na página da comissão

permanente das Universidades Federal e Federal Rural de Pernambuco, localiza no endereço *http://www.covest.com.br/institucional/sites.html*.

2.3.4 Atividades

O concurso vestibular segue as mesmas etapas e características previamente apresentada no processo de concursos públicos, na subseção 2.2.4.

2.3.5 Convocação e divulgação

O decreto número 2.306, publicado no *DOU* número 159, Seção 1, da página 17991, de 20 de agosto de 1997, define que as instituições de ensino superior anualmente, antes de cada período letivo, tornarão públicos seus critérios de seleção de alunos. Nesta ocasião também tornarão públicos o seguinte:

- A qualificação do seu corpo docente em efetivo exercício nos cursos de graduação;
- A descrição dos recursos materiais à disposição dos alunos, tais como laboratórios, computadores, acessos às redes de informação e acervo das bibliotecas;
- O elenco dos cursos reconhecidos e dos cursos em processo de reconhecimento, assim como dos resultados das avaliações realizadas pelo *Ministério da Educação e do Desporto*;
- O valor dos encargos financeiros a serem assumidos pelos alunos e as normas de reajuste aplicáveis ao período letivo a que se refere o processo seletivo.

Concursos vestibulares guardam grandes semelhanças com concursos públicos. Devido a essas semelhanças, pode-se adotar na etapa de convocação um modelo de edital semelhante ao apresentado para concursos públicos, conforme visto na subseção 2.2.5. Sugere-se aqui que o modelo contenha o seguinte:

1. Indicação - Edital, número e data;

2. Objeto do concurso - Onde é detalhada a disponibilidade de vagas por curso reconhecido;

3. Das inscrições:

    - Local;
    - Período;
    - Se a inscrição pode ser feita por procuração;
    - Reserva de vagas para minorias;
    - Uso do *ENEM*;

4. Da realização:

    - Local;
    - Cronograma das suas etapas;
    - Hora de comparecimento para ingresso no recinto;
    - Hora para início da avaliação;
    - Forma de ingresso;
    - Condições de realização da prova quanto a consulta bibliográfica, uso de máquinas e instrumentos em geral;

5. Do programa:

    - Indicando as disciplinas;
    - Discriminando os conteúdos que serão abordados;
    - Especificando a bibliografia básica que será adotada;

6. Do processo seletivo:

    - Discriminação das etapas;
    - Procedimentos de avaliação, tais como notas mínimas e peso das questões;

7. Correção:

    - Indicação dos métodos de correção para questões objetivas, de múltipla escolha e subjetivas;

8. Da classificação e dos recursos;

    - Critérios para classificação;
    - Critérios de desempate;
    - Afixação de gabaritos para fins de recursos, se for o caso;
    - Forma de apresentação de recursos;
    - Vista de prova pelos candidatos;
    - Procedimentos que devem ser seguidos para solicitar revisão;
    - Instância para julgamento de recursos;

9. Outras disposições:

    - Prazo para matrícula;

Não foram encontradas referências a leis que definem como deve ser realizada a etapa de divulgação, cabendo à instituição definir que veículos usará para divulgar a lista de aprovados.

2.3.6 Preparação

A preparação das provas é realizada por uma *banca elaboradora*. O processo precisa estar sob responsabilidade e supervisão de um *coordenador*, que deve realizar o seguinte: definir os objetivos, escolher os *membros da banca*, selecionar as questões que irão compor a avaliação e manter a avaliação segura até o início da distribuição. Os membros da banca elaboradora são responsáveis pela criação das questões. Sugere-se o seguinte conjunto de normas, que pode ser usado para reger esse processo e evitar que ocorra *vazamento* de informação:

- Os membros da banca elaboradora não devem ter contato entre si;
- O coordenador deve definir quantas questões cada membro da banca elaboradora deve criar;
- Cada membro da banca durante a preparação deve ter cuidado com o seguinte:
  - As questões sejam armazenadas de forma segura, ou seja, terceiros não podem ter acesso ao conteúdo das questões;
  - As questões tenham interpretação única;
  - As questões abranjam apenas o programa definido no edital;
  - As questões abranjam todo o programa definido no edital;
  - As questões sejam inéditas;
  - As questões sejam independentes entre si, ou seja, uma questão não deve depender de outra para sua comprenssão;
  - As alternativas sejam independentes entre si, ou seja, uma alternativa não deve depender da existência de outra para sua compreensão;
  - As questões devem ser enviadas para o coordenador de forma segura;
- O coordenador deve selecionar as questões que irão compor a avaliação e armazenar a avaliação de forma a evitar acessos não autorizados, normalmente em um cofre.

Dentro da avaliação é importante que se mantenha a independência entre questões e dentro das questões que se mantenha a independência entre alternativas, pois o *cordenador* pode trocar a ordem das questões ou eliminar questões. Seguindo as sugestões apresentadas pode-se concluir que o número de questões disponíveis (n) para uma avaliação será igual a quantidade de membros na banca (m) vezes a quantidade de questões (q) elaboradas por cada membro, ou seja, $n = m \times q$. Por exemplo, uma banca elaboradora constituída de 4 membros onde cada um destes elaborou 10 questões (p), tem-se $n = 4 \times 10$. A quantidade de provas possíveis com p questões é dada por $C_{n,p} = \frac{n!}{(n!)-p!}$ onde $C_{40,10} = \frac{40!}{(40!)-10!}$ sendo possível elaborar $3.075.990.524.006.400$ diferentes provas

[1]. Outra alternativa para este processo é resumida na figura 2.2, nesta alternativa os membros da banca elabora a avaliação em conjunto, aumentando a consistência e padronização da avaliação mas diminuindo o número de avaliações possíveis.

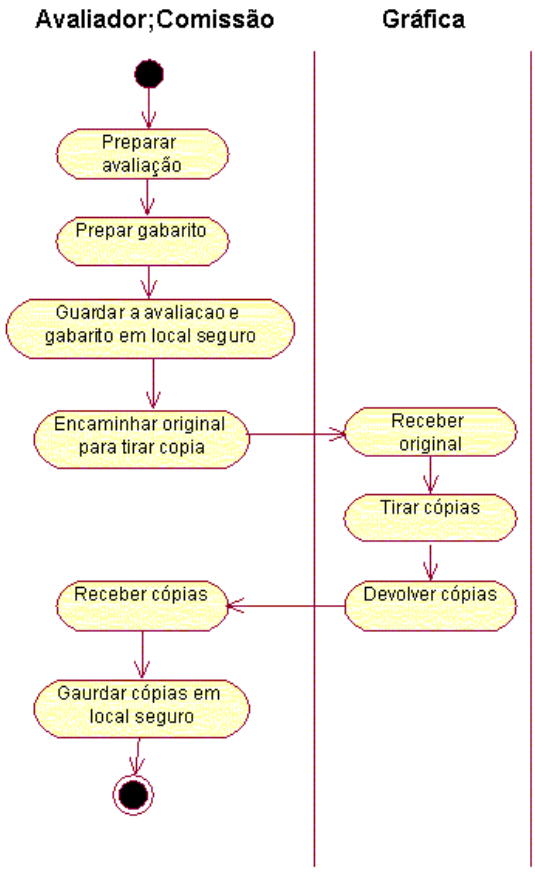

Figura 2.2: Seqüência do processo de preparação. Chama-se atenão para o fato de que as atividades executadas pela gráfica possuem pouca segurança. Como outra alternativa ao modelo apresentado nesta figura a comissão pode enviar as questões para um coordenador que ficará responsável pela segurança das questões e por definir quais questões farão parte da avaliação.

[1]Esta fórmula não excluí a possibilidade de uma avaliação conter questões elaboradas por um único autor.

2.3.7 Inscrição

A inscrição, assim como as demais etapas, deve ter seu funcionamento descrito no edital de convocação, a fim de garantir que o processo transcorra de forma transparente. É relativamente comum a disponibilização para o candidato de diversas formas para realizar a inscrição:

- Postos autorizados;
- Secretaria da instituição;
- Correios;
- Páginas na *internet*.

O processo de inscrição, resumido pela Figura 2.3, em algumas instituições vem já a algum tempo sendo feito através da *Internet*. Por exemplo, para o vestibular 2002 a *Universidade para Desenvolvimento do Estado de Santa Catarina*, ou simplesmente *UDESC*, disponibilizou em seu endereço na Internet, localizado em [UDE 01], um formulário para o processo de inscrição, onde o futuro candidato após preencher todos os campos é considerado pré-inscrito. O candidato pré-inscrito tem acesso a um boleto pagável em qualquer agência bancária. Seguido este processo deve-se enviar via *Sedex* para *UDESC* o formulário impresso ao final do processo de pré-inscrição, assinado e anexado a uma foto de $5cmX7cm$ datada do ano anterior, junto com uma fotocópia da cédula de identidade.

2.3.8 Aplicação

O processo de aplicação é executado seguindo as mesmas regras definidas para concursos, conforme descrito na subseção 2.2.8. O processo de aplicação pode ser dividido em dois subprocessos, onde no primeiro o avaliado é autorizado a participar da avaliação, conforme ilustrado na Figura 2.4, e no segundo o avaliado responde às questões da avaliação, como ilustrado na Figura 2.5.

2.3.9 Apuração

O processo de apuração, resumido na Figura 2.6, deve seguir os princípios da igualdade e impessoalidade. De forma geral, para garantir estes princípios a *banca corretora* não deve possuir acesso ao nome do candidato. Testes de múltipla escolha podem ser corrigidos por computadores. O Edital deve determinar, sempre que possível, como será procedida a correção dos cartões de respostas. Os itens serão considerados errados e, portanto, não computados como acertos, quando ocorrer um ou mais do seguinte:

- A resposta assinalada pelo candidato for diferente daquela listada como correta no gabarito;
- O candidato assinalar mais de uma opção para cada questão;
- O candidato deixar de assinalar alguma opção;
- Ou houver rasuras.

Para provas subjetivas, os critérios adotados para avaliação devem, preferencialmente, ser definidos no edital. A correção das provas, bem como a apuração da nota final, devem ser feitas sem identificação nominal dos candidatos, garantindo desta forma o princípio da impessoalidade. Merece destaque o trabalho realizado pela *Convest*, em [CON 02], que introduziu no ano de 2000 diversos mecanismos para impedir a identificação das provas discursivas pelos corretores. O processo adotado denomina-se *correção cega*. O principal mecanismo desse processo é a identificação de cada prova por um código, que pode ser lido por um leitor óptico. As notas são lançadas em uma ficha para leitura óptica e não no caderno de respostas do candidato. Cada prova recebe duas notas que podem ser dadas em tempos distintos, sendo que o segundo corretor não tem conhecimento da nota atribuída pelo primeiro. Após a atribuição é feito o processamento pela equipe de informática. Realizado o processamento, emite-se uma série de relatórios periódicos que apontam as discrepâncias entre as notas dos dois corretores. A média das duas notas foi adotada como nota final quando a diferença das duas for, no máximo,

um ponto; no caso de uma diferença maior do que um ponto será realizada uma terceira correção. O processo de *correção cega* foi adotado visando fornecer maior tranqüilidade ao avaliado com relação a lisura do processo. As questões de múltipla escolha são corrigidas por sistemas computacionais.

2.3.10 Classificação

Os resultados são ordenados de forma que seja simples demonstrar os melhores candidatos. De forma geral, tem-se o processo ilustrado na Figura 2.7. A [CON 02] acrescenta a esta atividade a análise do desempenho dos candidatos, para determinar índices que permitam definir a qualidade das questões e da avaliação. Por exemplo, a [CON 02] analisa o seguinte para cada questão que compõem a avaliação:

- **IF - Índice de facilidade** - Mede o quanto a questão foi fácil, ou difícil, para o conjunto de indivíduos que se submeteram a uma determinada avaliação. O índice varia entre 0 e 1 e quanto mais próximo de 1 mais fácil é a questão;
- **ID - Índice de discriminação** - Mede o quanto uma determinada questão é capaz de separar os candidatos que obtiveram melhor desempenho na prova daqueles de pior desempenho. Ou seja, um item discriminativo é respondido corretamente pelos candidatos de melhor desempenho na prova e incorretamente pelos candidatos de pior desempenho;

A Universidade Federal do Rio Grande do Sul (*UFRGS*) procura por *cola*, medindo a quantidade de coincidências entre candidatos. Ou seja, procura localizar candidatos que cometeram os mesmos erros e acertos nas provas objetivas.

2.3.11 Publicação

Atualmente as instituições em sua grande parte adotaram a *Internet* como um canal para divulgação dos resultados. Quando, por exemplo, a Unicamp publica a relação dos classificados, a página *Internet* correspondente tem seu maior índice de acesso no ano. Por exemplo, com o anúncio dos classificados no dia 20 de dezembro de 2001,

aconteceram cerca de 300 mil consultas dos dados disponíveis em [ACA 02]. No entanto, o resultado ainda continua sendo divulgado pela imprensa escrita.

2.3.12 Revisão

Sugere-se o uso das mesmas idéias esplanadas na subseção 2.2.12 em conjunto com o processo que pode ser visto na Figura 2.8.

Os seguintes serviços são normalmente automatizados:

- Processamento das correções de provas;
- A preparação das listas de convocados para matrícula;
- A geração das listas de convocados e de espera e o processamento das matrículas.

2.4 Certificações

Um treinamento agrega conhecimento e desenvolve habilidades, através deles as empresas repassam conhecimento e procuram melhorar seu quadro pessoal. Porém o processo de treinamento empresarial precisa de garantias de efetividade para evitar que ocorram: acidentes, perdas de produtividade, desperdícios e falta de qualidade. Um processo de certificação pode ser usado para demonstrar o nível de conhecimento de uma pessoa, isto é, ao passar em um exame a pessoa comprova o quão apta está para realizar uma determinada atividade.

A empresa ou organização proprietária do produto ou tecnologia para o qual a certificação foi desenvolvida atesta a qualificação da pessoa, emitindo um certificado. Na área técnica tem-se como exemplo grandes empresas que possuem programas de certificação como: Oracle, Microsoft, Sun e Novell.

2.4.1 Tipos de Certificações

As certificações podem ser agrupadas em:

- Licenciamento profissional;
- Licenciamento (como, por exemplo, carteira de motorista);
- Certificação profissional;
- Certificação Acadêmica.

2.4.2 Estudo de caso

A Prometric é líder mundial em fornecer tecnologia de Avaliação do Conhecimento, providenciando tecnologia para aplicação em empresas que lidam com grandes volumes de avaliações e/ou avaliados. Com um faturamento em 2001 de $7,2$ bilhões de dólares oferece os seguintes serviços:

- Preparação de avaliações;
- Processamento dos resultados;
- Consultoria na preparação;
- Marketing das certificações.

As avaliações são realizados em unidades certificadoras que são autorizadas pela Prometric, no Brasil existem entidades certificadoras nas capitais e grandes centros. A Prometric, por sua vez, é autorizada por empresas ou grupos a emitir certificados que devem ser autenticados pelas unidades certificadoras através de carimbo, marca d'água de assinatura de pessoa autorizada pela Prometric. A atuação da Prometric encontra-se dividida em três grandes segmentos:

Empresas de tecnologia, onde destacam-se como clientes: Cisco, Compaq,IBM, Microsoft, Oracle;

Acadêmica, onde destaca-se como cliente *Educational Testing Service's* ou *ETS* responsável por diversos testes acadêmicos nos Estados Unidos como, por exemplo, o teste de proficiência em língua Inglesa (*Test of English as a Foreign Language - TOEFL*);

Licenciatura profissional, onde existem exames para mais de 70 organizações como, por exemplo, *National Association of Securities Dealers*;

2.4.2.1 Princípios

Credibilidade é o principal beneíficio da certificação, pois as empresas acreditam que os profissionais certificados comprovaram domínio. Segundo a Prometric 85% dos empregadores pagam pela avaliação do seu pessoal.

2.4.3 Equipe

A Prometric possui profissionais na área de preparação, correção e centros autorizados que empregam *administradores* que na realidade são responsáveis pelo processo de fiscalizaç ao da aplicação.

2.4.3.1 Infra-estrutura

No ano de 2001 a empresa, que tem sede em Baltimore nos Estados Unidos, disponibilizou 2400 diferentes testes através de uma estrutura que consiste de 4800 centros autorizados para realização de testes. Existem filiais em 136 países, empregando mundialmente 3000 pessoas. Cada certificadora possui no mínimo:

- Uma sala de uso individual, dispondo de acomodações em geral;
- Computador com acesso a rede, sem nenhuma unidade de disco removível (disquete, gravador de cd ou outra mídia), software de avaliação instalado;
- Dicionário;
- Papel e lápis;
- Uma câmera que monitora o avaliado durante todo o processo;

A sala de teste é de uso individual sendo circundada por vidro transparente.

2.4.4 Atividades

Tipicamente o processo de uma certificação segue a mesma seqüência de atividades de um concurso, ou seja, é necessário: divulgar, elaborar, distribuir, avaliar e corrigir.

2.4.5 Divulgação

As empresas podem criar sua própria campanha de marketing ou adquirir este serviço da Prometric. Os salários recebidos pelas pessoas que possuem algumas certificações, como as da Microsoft, em muitos casos são usados como fator motivante nestas campanhas.

2.4.6 Distribuição

A avaliação é feita dentro de uma sala de uso individual em um computador que possui o software de avaliação instalado. Um dia antes da avaliação o administrador do sistema, que faz também o papel de responsável pela assinatura do certificado conecta-se a Prometric através do software e envia a lista de provas e candidatos do dia seguinte. Na manhã em que o teste será realizado é feita uma conexão que faz a transferência das provas que serão aplicadas no dia, o canal usado tem sua segurança garantida através do uso de algoritmos criptográficos, como os descritos no capítulo 5, infelizmente não são fornecidas informações sobre o algoritmo usado para que se possa determinar sua efetividade. Mesmo que dois candidatos estejam agendados para fazer a mesma avaliação em um determinado dia não se pode garantir que as provas serão iguais, pois o servidor realiza um sorteio prévio das questões, a quantidade média de questões disponíveis no servidor por prova não esta publicada.

2.4.7 Avaliação

Para realização da avaliação o avaliado deve entrar em contato com uma unidade autorizada e indicar qual teste irá fazer e em qual data estará fazendo este. O

processo de avaliação é bastante simples:

I. Primeiro é verificada a identidade do candidato, que deve possuir um documento que contenha foto. Em alguns casos esta etapa requer que seja apresentada uma carta de autorização da empresa que está patrocinando a avaliação. Em outros, uma foto digital é enviada à empresa do cliente;

II. Todos os itens pessoais dos candidatos devem ficar fora da área de teste;

III. Em vários exames, é providenciado papel de rascunho e lápis. O papel usado deve ser timbrado, carimbado, e devolvido ao sair da sala.

O administrador do centro autorizado pode a qualquer momento cancelar a pontuação e a avaliação quando houver por parte do avaliado:

I. Comportamento inapropriado;

II. Impossibilidade de comprovar a identidade;

III. Tentativa de fazer o teste no lugar de outra pessoa;

IV. Tentativa de receber auxílio;

V. Tentativa de remover o rascunho da sala de avaliação;

VI. Tentativa de usar material fora o que foi deixado na sala pelo administrador;

VII. Tentativa de remover questões em qualquer formato da sala de avaliação;

VIII. Tentativa de obter acesso não autorizado ao teste, a questões do testes ou informações não públicas sobre o teste;

IX. Tentativa de permanecer na sala de avaliação por mais tempo do que o permitido;

O número de questões nas avaliações varia entre as diversas certificações oferecidas, por exemplo, a certificação de *Programador Java* é constituída de 60 enquando a de *Desenvolvedor Java* contem apenas 5 questões. As questões são em sua maioria de múltipla escolha, em poucas questões é necessária a digitação de alguma resposta e

quando isto é necessário limita-se normalmente a digitação de algumas poucas palavras. Têm-se, exceções como o caso da avaliação de *Desenvolvedor Java* que, por este motivo, será detalhada na seção 2.4.8.

2.4.7.1 Correção

As avaliações, normalmente, são corrigidas pelo *software* que emite um certificado contendo o resultado do aproveitamento¿ O certificado é impresso em papel especial e logo em seguida carimbado e assinado. O certificado emitido no *TOEFL* quando realizado por computador contém uma foto tirada do avaliado no momento da avaliação por uma câmera fixada no computador.

Na *certificação de Desenvolvedor Java*, detalhada na seção 2.4.8, o resultado não é corrigido pelo computador e sim encaminhado para uma empresa independente especializada em corrigir este e outros testes relacionados a área de tecnologia.

2.4.7.2 Segurança

A Prometric distribui suas avaliações a partir de um computador central através de uma rede de computadores. A avaliação é distribuída por um canal seguro, conforme apresentado em 2.4.6, as avaliações são armazenadas cifradas. As avaliações ficam na memória do computador em formato aberto apenas durante a avaliação. Regularmente são realizadas checagens de segurança no computador central, localizado na sede da Prometric, onde as questões permanecem todo tempo cifradas. Auditorias podem ser feitas nas autorizadas sem aviso prévio.

2.4.8 Certificação com Avaliação não Presencial

A certificação de *Desenvolvedor Java* diferencia-se das demais por estar dividida em duas etapas, sendo, uma prática não presencial e outra teórica feita de forma presencial:

- A prova prática é definida pela Sun que libera para o candidato a especificação de um projeto, quando se recebe a especificação pode-se iniciar a construção de uma

aplicação que atenda as características determinadas nas especificações do projeto. O candidato a desenvolvedor após finalizar o projeto deve enviar o código fonte deste para a Sun.

- A prova teórica pode ser feita se o candidato atingir na prova prática uma nota mínima. A prova teórica é constituída de cinco perguntas divididas em quatro partes. Esta prova diferencia-se também das demais por ser escrita, onde o candidato descreve suas decisões de implementação. Finalizado o teste não é emitido um certificado, apenas um documento indicando que as questões serão corrigidas e em breve será enviado o resultado.

O teste teórico é aplicado para determinar se o avaliado foi realmente o desenvolvedor da aplicação, pois acredita-se que se ele sabe responder perguntas sobre a aplicação ele deve ter criado esta.

2.5 Avaliação Presencial em Sala de Aula

Segundo [VAS 98], "O ensino tem que ser muito exigente, já que nós queremos apenas transformar o mundo". As avaliações, como normalmente vêm sendo aplicadas, obrigam que os avaliados estejam durante a avaliação na presença do avaliador e sob constante supervisão. O avaliado tem que, por exemplo, se deslocar de sua residência para um local previamente definido, onde ocorrerá a avaliação. Em [VAS 98], lembra-se a existência de diversos fatores geradores de tensão e dificuldades. Exemplificam-se estes fatores abaixo:

- Data marcada;
- Horário rígido quanto ao início;
- Horário rígido quanto à duração;
- Matéria determinada;
- Relação de desconfiança;

O professor ao desejar que o aluno seja muito bom e muito competente deve estar durante todo o processo avaliando a aprendizagem para poder determinar a qualidade do seu trabalho e o aproveitamento do grupo. Com base nos resultados cabe ao professor repensar sua postura e procurar corrigir os problemas que venham a surgir, podendo levar novas atividades com o mesmo conteúdo que permitam superar as dificuldades, e este conteúdo deve fazer parte da próxima avaliação para verificar se as dificuldades foram superadas [VAS 98]. No entanto, a efetividade e validade da avaliação, segundo [VAS 98], dependem de uma rápida correção e devolução dos resultados. Ao aplicar avaliações contínuas ele, o professor, acaba se sobrecarregando [VAS 98] e para evitar o excesso de trabalho muitos professores optam por aplicar um número reduzido de avaliações, onde os alunos são avaliados em uns poucos momentos. Reduz-se desta forma o desgaste do professor, mas tem-se menor retorno sobre o real aproveitamento do grupo [VAS 98, AVA 98].

2.5.1 Papéis da Avaliação

Liane Tarouco, em [TAR 00], enfatiza que como a avaliação está normalmente desvinculada do processo de ensino e aprendizagem esta acaba servindo apenas para classificar o aluno e fica sem repercussão na dinâmica de trabalho adotada em sala de aula. O trabalho de [MAD 71], conforme [TAR 00] , caracteriza a avaliação como dos três tipos seguintes:

Formativa - Executada durante o processo de instrução incluindo todos conteúdos importantes da etapa; sendo útil como forma de fornecer ao aluno retorno sobre o que este realmente aprendeu e o que precisa aprender. O professor por sua vez é beneficiado com a rápida identificação do seguinte:

- Falhas dos alunos;
- Aspectos que devem ser modificados;
- Atendimento às diferenças individuais dos alunos;
- Medidas alternativas para recuperação das falhas de aprendizagem;

Somativa - Executada ao final da instrução, com o objetivo de verificar o que o aluno efetivamente aprendeu; neste tipo de avaliação procura-se o seguinte:

- Incluir os conteúdos mais relevantes;
- Contemplar os objetivos mais amplos do período de instrução;
- Fornecer um meio do aluno conhecer seu desempenho;
- Atribuir notas aos alunos;
- Permitir comparar diversos alunos;

Diagnóstica - Antes e durante o processo de instrução, onde no primeiro momento tem por funções o seguinte:

- Verificar se o aluno possui determinadas habilidades básicas;
- Determinar se objetivos de um curso já foram dominados pelo aluno;
- Agrupar alunos conforme suas características;
- Encaminhar alunos a estratégias e programas alternativos de ensino;

Em um segundo momento procura-se buscar a identificação das causas não pedagógicas dos repetidos fracassos de aprendizagem, promovendo, inclusive quando necessário, o encaminhamento do aluno a outros especialistas tais como psicólogos e orientadores educacionais, entre outros.

Fica claro em [TAR 00], que apesar de poderem existir diferenças estruturais entre testes formativos, somativos e diagnósticos, todos os três podem servir às três funções da avaliação, dependendo do uso que se pretenda fazer dos seus resultados. Sem o uso de avaliações não há como tomar decisões que visem a melhoria do processo ensino-aprendizagem.

2.5.2 Princípios

Os princípios da igualdade e impessoalidade, por questões morais devem ser seguidos pelo avaliador. Apesar de estudos comprovarem que o avaliador tende a ser mais rígido nas últimas avaliações que corrige de um grupo de avaliados.

2.5.3 Equipe

É comum que uma única pessoa, o professor do curso ou disciplina, realize todas as atividades das avaliações. Em alguns casos a atividade de revisão é realizada por uma banca de professores como pode ser visto em 2.5.11.

2.5.4 Infra-estrutura

O ambiente usado para ensinar costumeiramente também é usado como espaço físico para aplicação da avaliação, no entanto, dependendo do caso o avaliador tem plena liberdade para escolher outro ambiente. Pode-se terceirizar ou possuir equipamentos e equipe para reproduzir a avaliação.

2.5.5 Atividades

As etapas seguem a mesma lógica e seqüência enumeradas para outras avaliações, sendo assim necessário: divulgar, elaborar, aplicar, apurar (*corrigir*), publicar os resultados e revisar.

2.5.6 Convocação e Divulgação

Avaliações formativas, somativas ou diagnósticas devem ter antes de aplicados suas regras especificadas e objetivos definidos. Deve-se divulgar e esclarecer amplamente para os avaliados estas regras e objetivos. A definição e divulgação ocorrem inclusive nos chamados testes ”surpresa”, onde a divulgação é realizada com pouca ou nenhuma antecedência. Sugere-se que na divulgação seja indicado:

1. Objetivo da avaliação;
2. Da execução:
    (a) local;
    (b) data da realização;

(c) período, ou seja, horário de início e de término;

(d) condições de realização quanto a consulta bibliográfica, uso de máquinas e instrumentos em geral;

3. Do Programa:

(a) indicando os conteúdos;

(b) especificando a bibliografia básica que será adotada;

(c) peso desta na composição da nota final do avaliado dentro do período ao qual a avaliação se refere;

4. Da correção:

(a) indicação dos métodos de correção para questões objetivas, de múltipla escolha e subjetivas;

(b) vista de prova;

(c) forma de apresentação de solicitação de revisão;

Normalmente são considerados aptos a participar e inscritos todos os *alunos* do curso ou disciplina para a qual está sendo realizada a avaliação.

2.5.7 Preparação

A preparação das avaliações é realizada pelo professor que, baseado em seu objetivo, no conteúdo ministrado e nos seus conhecimentos define as questões que irão compor a avaliação. Cabe ao próprio elaborador manter a avaliação segura até o início da distribuição. Foge ao escopo deste trabalho apresentar técnicas para preparação de questões.

2.5.8 Aplicação

Na data e hora definidas o avaliado deve comparecer ao local designado para a realização da avaliação, onde o avaliador identifica os avaliados, normalmente, sem

nenhuma checagem formal da identidade. Dependendo das regras da instituição, antes do início os presentes devem assinar uma ata, que serve como comprovante de presença e de entrega da avaliação. Durante a realização da avaliação não se costuma admitir qualquer espécie de consulta ou comunicação entre os avaliados ou destes com outras pessoas seja diretamento ou através do uso de aparelhos que possiblitem o recebimento de mensagens. Consulta a materiais ou equipamentos mecânicos ou eletrônicos que operem resultados podem ser permitidos em algumas avaliações, dependendo das regras estabelecidas pelo avaliador. O avaliado pode ter sua pontuação eliminada total ou parcialmente, dependendo das regras definidas pela instituição, quando:

I. Utilizar ou tentar utilizar de meios ilícitos para a resolução da avaliação;

II. Contrariar qualquer uma das regras que foram definidas;

III. Contrariar determinações do avaliador;

IV. Cometer qualquer ato de indisciplina durante a realização das provas;

V. Faltar a na avaliação;

VI. Chegar ao local de avaliação após qualquer um dos avaliados entregar a avaliação e se retirar do local de avaliação;

O fiscal não pode ficar sozinho com nenhum dos avaliados durante o período que a avaliação estiver sendo executada, devendo permanecer com ele no mínimo três avaliados. Para evitar dúvidas sugere-se que, as regras adotadas sejam definidas no edital do concurso.

2.5.9 Apuração

O processo de apuração deve seguir os princípios da igualdade e impessoalidade, no entanto normalmente em cursos, ou disciplinas de escolas e faculdade não são empregadas técnicas que impossibilitem o corretor de ter conhecimento da identidade do avaliado, o que pode tornar a avaliação subjetivo e sujeita a pré-julgamento.

2.5.10 Publicação

A maneira mais simples de divulgar os resultado é a entrega da avaliação para que o avaliado possa verificar seus erros e acertos. Também é possível que o avaliado possa verificar seu aproveitamento, por exemplo, através de: comunicação verbal, fixação do resultado em local público, disponibilização em uma página na Internet, comunicação do resultado por e-mail ou correspondência. Não existe nenhuma restrição quanto ao uso de mais de um dos meios listados.

2.5.11 Revisão

Após os avaliados verificarem a correção que foi feita pelo avaliador podem surgir dúvidas sobre a correção como, por exemplo, considerar que alguma ou algumas questões tiveram seu valor atribuído de forma errada. Dependendo da instituição e de regras definidas este problema pode ser verificado e sanado, se necessário, por uma comissão que se reúne especificamente para resolver estes casos ou diretamente pelos envolvidos, avaliador e avaliado.

2.6 Conclusão

A execução bem sucedida de uma avaliação, vide figura 2.9, depende diretamente da definição e execução do processo de avaliação a partir de regras bem definidas. Para um ambiente onde a aplicação seja aplicada usando computadores e a Internet como canal este trabalho adota os conceitos apresentados neste capítulo e usa os princípios, processos e regras adotados para realização de concursos públicos nos demais tipos de avaliação. Esta adoção não prejudica os demais tipos de avaliação e adiciona a elas critérios e regras que ajudam o processo a transcorrer de forma clara e padronizada. As informações aqui são aplicadas no capítulo 6, onde é definido um protocolo para *segurança na avaliação não presencial*.

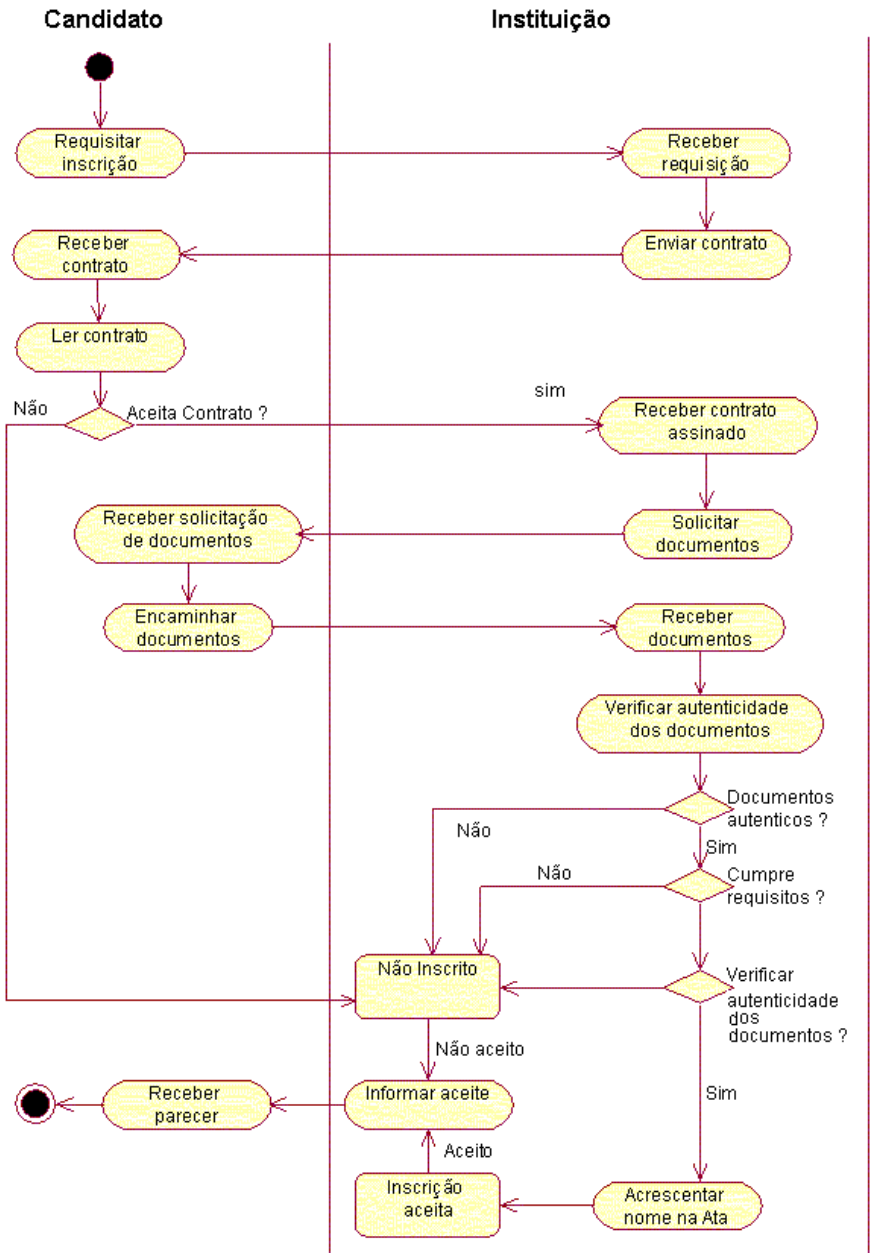

Figura 2.3: Seqüência do processo de inscrição. Neste diagrama o candidato é uma pessoa qualquer que pode preencher ou não os requisitos legais, quando o candidato requisita sua inscrição ele é considerado pré-inscrito. Quando o candidato entrega a documentação e a instituição considera que a documentação esta correta o candidato passa a ser considerado inscrito.

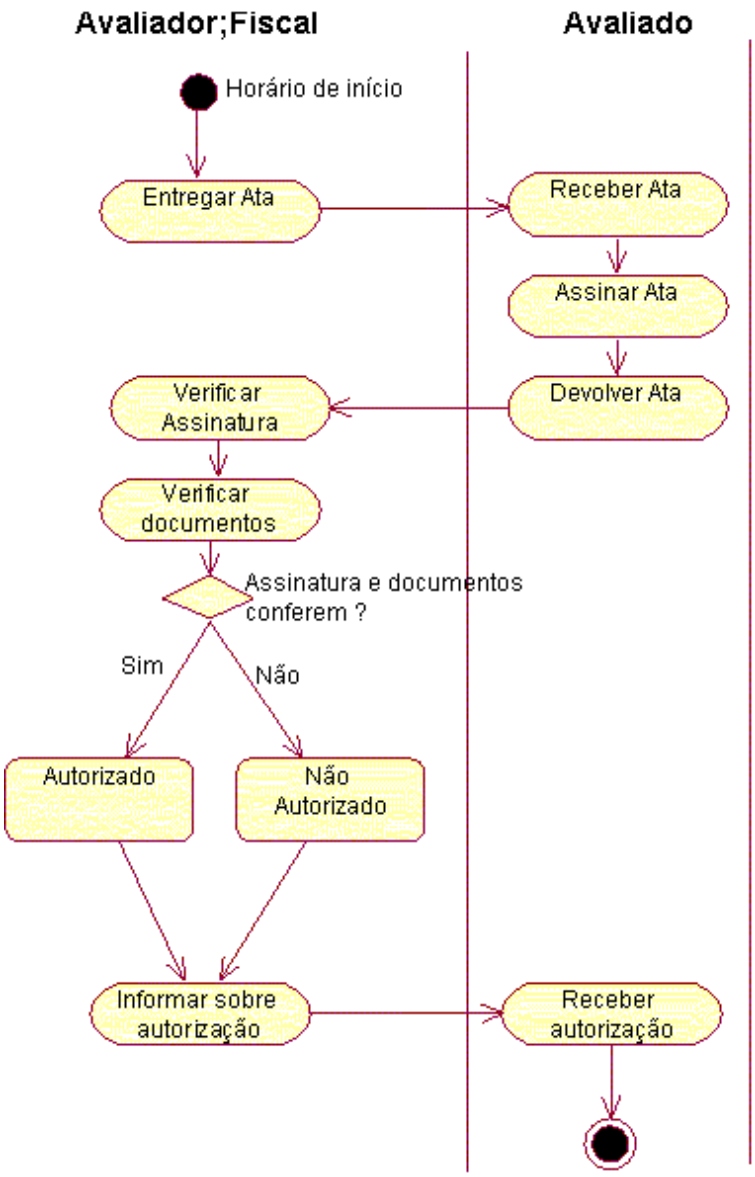

Figura 2.4: Seqüência da autorização para participação da avaliação.A avaliação inicia quando o fiscal autoriza a entrada do avaliado no local de avaliação.

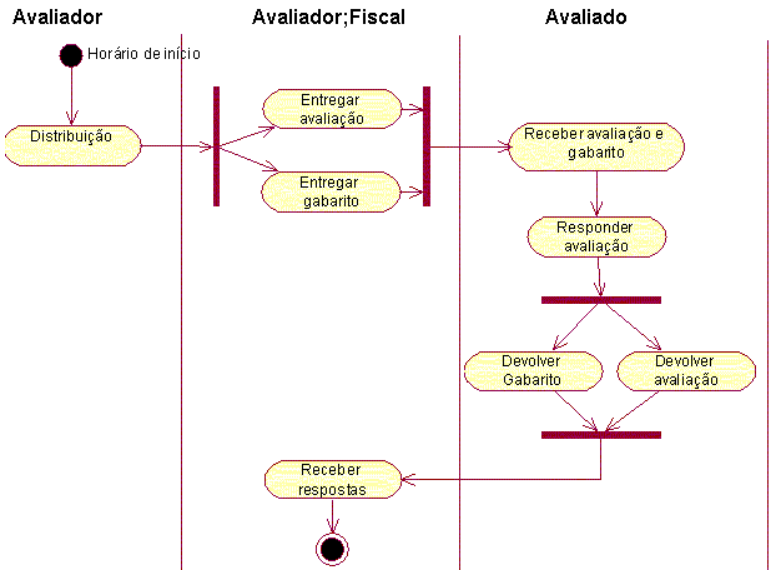

Figura 2.5: Seqüência da execução da avaliação. Cabe ao coordenador ou ao avaliador ou ao presidente a responsabilidade sobre o processo logístico de distribuição das avaliações. O fiscal, por sua vez, fica responsável por controlar cada um dos avaliados durante o processo.

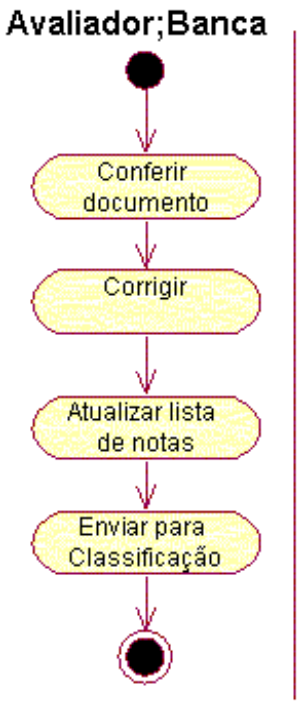

Figura 2.6: Seqüência do processo de apuração. A tarefa de correção é o cerne do processo de avaliação, e deve primar pela impessoalidade dos valores atribuídos as respostas dadas pelos candidatos

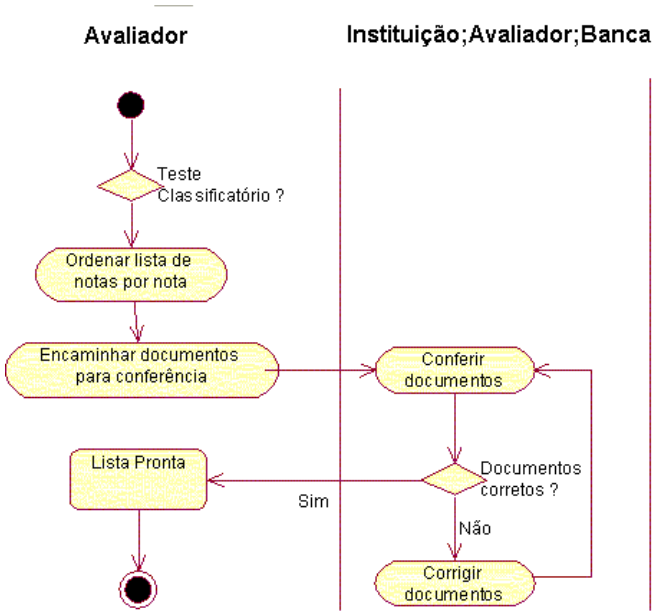

Figura 2.7: Seqüência do processo de classificação

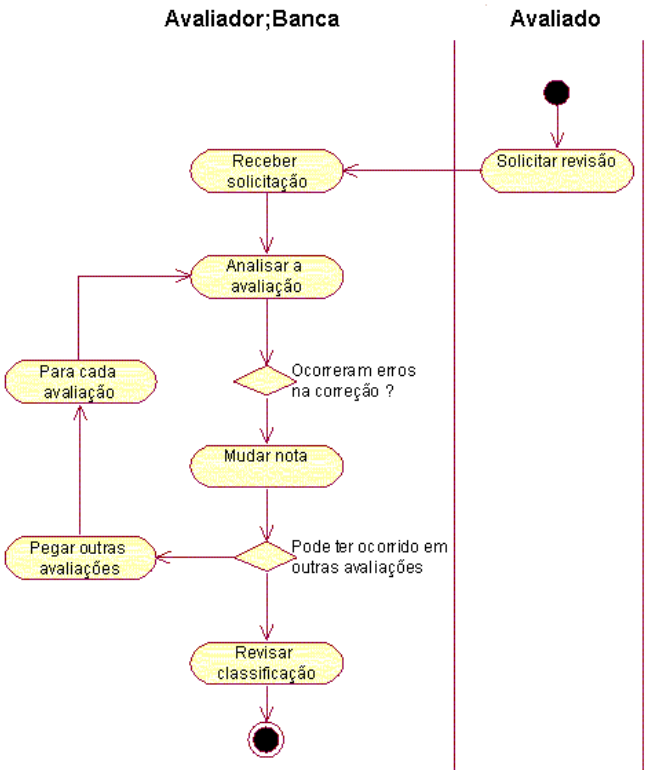

Figura 2.8: Seqüência adotada para revisão

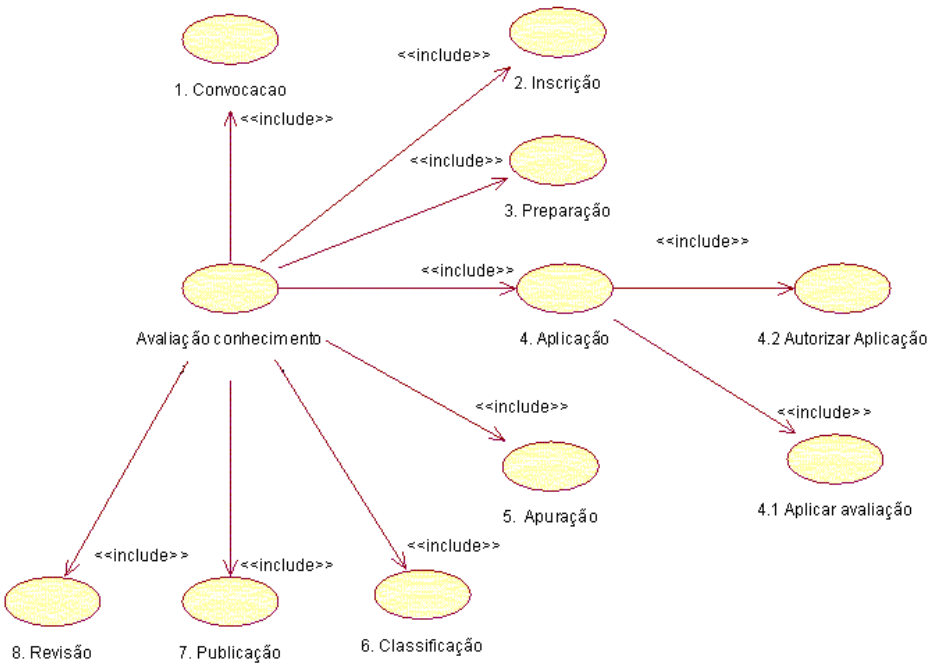

Figura 2.9: Composição do processo de avaliação. O processo de avaliação do conhecimento pode ser visto como a agregação de diversos sub-processos. Estes sub-processos podem ser observados na leitura das descrições feitas anteriormente em: concursos 2.2, vestibulares 2.3, certificações 2.4 ou em avaliações em sala de aula 2.5.

Capítulo 3

Ensino a Distância

3.1 Introdução

Em [dINE 98, SPO 96] define-se ensino a distância como uma forma de educação onde há uma separação entre professor e aluno, onde tecnologias de comunicação são usadas para resolver o problema de distância. [SPO 96] completa afirmando que esta definição torna-se incompleta se não for considerada que, além da separação no espaço, existe também uma separação no tempo. A separação no tempo é classificada no trabalho de Ribeiro, [dINE 98], usando o clássico *4-Square Map of Groupware Options* desenvolvido por [JOH 91] representado na figura 3.1 e detalhado pela descrição:

Mesmo horário/Mesmo local: reuniões face a face; por exemplo, aulas presenciais;

Mesmo horário/Local diferente: reuniões virtuais com uso de um meio de telecomunicação ou teleconferência, ferramentas de *chat*;

Horário diferente/Mesmo local: os estudantes comparecem em diferentes instantes de tempo para interagir com os instrutores e/ou ferramentas;

Horário diferente/Local diferente: usa tecnologias que permitem comunicação assíncrona.

Através do trabalho de [SPO 96] percebe-se de forma cristalina que o ensino a distância é um produto da tecnologia, e que este produto nasceu da união da

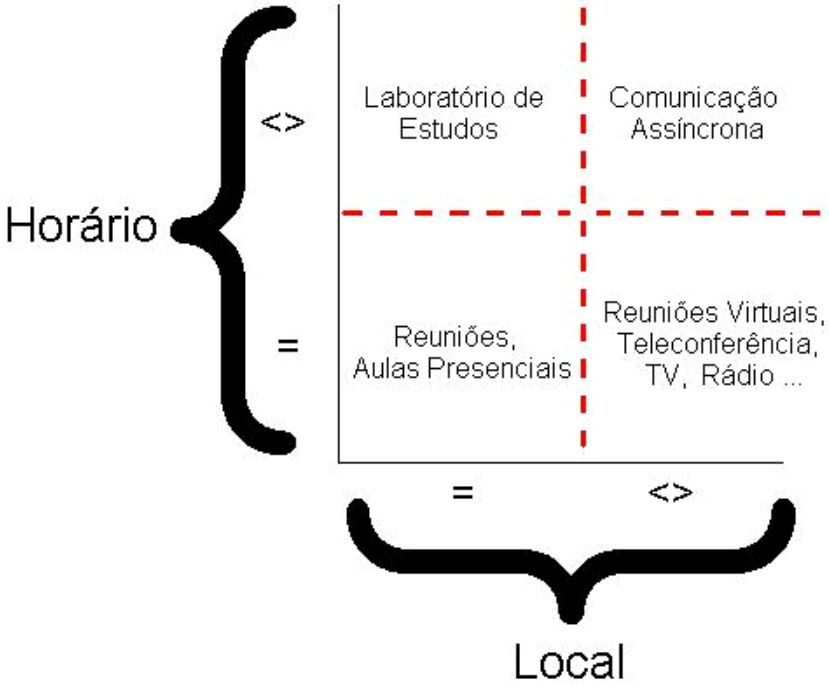

Figura 3.1: 4-Square Map of Groupware Options. Cursos com auxílio da Internet podem se posicionar em qualquer ponto do quadrado, o fator determinante neste posicionamento são os objetivos, a modelagem e tecnologias escolhidas.

invenção da imprensa por Gutenberg e o surgimento dos correios globais. O ensino tradicional e o ensino a distância puderam tornar-se muito mais didááticos com o apoio das transmissões por rádio, televisão e pelo desenvolvimento dos fonógrafos, fitas de audio e fitas de vídeo. No entanto, nenhuma destas tecnologias pôde fornecer meios para que o aluno interagisse com o professor e outros alunos.

A real dimensão do processo de avaliação e sua importância, dentro do amplo processo de ensino a distância, só podem ser observadas com uma base de conhecimento do processo. Para isto, mostra-se neste capítulo a origem, a importância que o ensino a distância exercerá no futuro do nosso país e as deficiências que ainda são encontradas neste no que se refere à avaliação do conhecimento a distância. O capítulo fornece uma visão sobre a origem do ensino a distância, seção 3.2, e enfatiza os problemas deste tipo de ensino (3.3) e apresenta informações sobre o foco adotado pela maioria dos

pesquisadores (3.4) finalizando com uma breve descrição da nossa legislação (3.5).

3.2 Origem do Ensino a Distância

Conforme [BER 98] os primeiros registros da utilização de Treinamentos a Distância que se tem conhecimento são datados de 1900, onde no Alaska, as indústrias de mineração utilizavam-se esta forma de repasse de conhecimento, para treinar mineradores em escavação no gelo. Os mineradores estavam separados geograficamente em uma região com topografia extremamente acidentada, assim, estes treinamentos foram disponibilizados através de correspondência pela "Colliery Engineer School of Mines".

A primeira utilização de rádio para repasse de treinamento foi em 1925 pela Universidade Estadual de Iowa para disponibilização de créditos de graduação. Na década de 1940 à 1970, a televisão começou a ser utilizada como ferramenta educacional iniciando com a Universidade Estadual Iowa em 1951. A partir da década de 80, com a popularização dos PCs, começaram a ser desenvolvidos os treinamentos suportados por tal tecnologia. Porém, o primeiro registro de utilização de computadores para treinamentos data de 1969 com um treinamento sobre Sistemas de Mainframe na IBM.

3.3 O Problema da Comunicação

Até o advento das tecnologias de telecomunicação, educadores de cursos a distância ofereciam interação bidirecional por correspondência, o que forçava a independência do aluno pois o principal meio de instrução era o papel impresso, geralmente entregue usando serviço postal. Com o desenvolvimento de tecnologias interativas bidirecionais de tempo real, tais como áudio, teleconferência e vídeoconferência, tornou-se possível unir instrutores e estudantes que estão separados geograficamente usando interação em tempo real. Essas tecnologias não se demonstraram muito adequadas para promover aprendizagem em grupo, sendo adequadas para comunicação um-para-um, de acordo com [dINE 98]. O ensino com auxílio do computador sem levar em consideração as tecnologias para internet sofria destes mesmos problemas de comunicação e podia de

forma extremamente genérica ser dividido da seguinte forma:

- **CAI - computer-assisted instruction** O uso de computadores como ferramentas de suporte ao ensino;
- **CMI - computer managed instruction** O uso de computadores para registrar: alunos, grades de horário, controlar e guiar o processo de aprendizado, e analisar e reportar desempenho;
- **CBT - computer based training** O uso de programas instrucionais, também denominados de lições, que são controlados por sistemas CMI;

A Internet como canal para aplicação do Ensino a distância quando adequadamente usada consegue fornecer interação entre alunos e professores em tempo real de muitos-para-muitos. Com o uso da internet consegue-se uma maior colaboração através do uso de ferramentas como: e-mail, WWW, listas de discussão, videoconferência.

3.4 Projetos na Área de Ensino a Distância

Apesar de estarmos agora no momento em que educadores reconhecem o grande potencial do uso da Internet para aumentar a qualidade dos cursos oferecidos nos campus [DRI 98] a maioria dos projetos de ensino tem-se focado nos aspectos didáticos como observados por [OLI 00, ISE 00, GIU 00]. Enquanto os aspectos ligados à tecnologia em muitos casos são relegados a um segundo plano ou considerados muito complexos como em [DRI 98, ISE 00]. Sendo poucos projetos relacionados aos aspectos de segurança como é o de [FIO 00]. O IEEE possui atualmente um grupo de trabalho voltado para a área de aprendizado, o grupo denomina-se “IEEE Learning Technology Task Force” onde o subgrupo IFET “International Forum of Educational Technology” possuindo como principal objetivo incentivar os debates sobre o uso da tecnologia no ensino e divulgar artigos, teses e recursos através do seu “site” e jornal.

Chadwick, [SPO 96], tem-se ainda um mercado que em 1995 contava com 300.000 pessoas engajadas no desenvolvimento nos Estados Unidos.

3.5 Legislação Brasileira

"Acompanhando o tom dos dados estatísticos, iniciativas como a criação da Secretaria de Governo de Educação à Distância, em maio de 1996; e os artigos sobre educação a distância foram incluídos na Lei de Diretrizes e Bases" [ECO 99]. A educação presencial conta, segundo censo escolar realizado com o MEC em 1998, com 45 milhões de alunos, o que corresponde a um terço da população brasileira.

O apoio governamental dá-se com a criação da Lei de Diretrizes e Bases da Educação Nacional, determinando que, o Poder Público incentivará o desenvolvimento e a veiculação de programas de ensino a distância, em todos os níveis e modalidades de ensino e de educação continuada. A determinação está regulamentada por:

Decreto número 2.494, de 10 de fevereiro de 1998 que regulamenta o artigo 80 da LDB (Lei número 9.394/96);

Decreto número 2.561, de 27 de abril de 1998 que altera a redação dos artigos 11 e 12 do decreto número 2.494;

Portaria número 301, de 7 de abril de 1998 que normatiza os procedimentos de credenciamento de instituições para a oferta de cursos de graduação e educação profissional tecnológica a distância.

3.6 Internet como Canal no Ensino a Distância

A importância do uso da internet como canal para ensino a distância conforme apontado por [CUN 00, DRI 98, BER 98, dVLHMG 00] deve-se principalmente a:

- Redução do custo logístico;
- Redução da quantidade de material impresso;
- Eliminação da necessidade de empacotar e transportar material;

- Eliminação da necessidade de manter ou alugar salas de aula;
- Diminuição dos custos com transporte e hospedagem de instrutores;
- Ampliação da velocidade de distribuição do conhecimento;
- Simplificação da correção de avaliações;
- Simplificação da atualização do material ditático, que pode facilmente ser distribuído para todos;
- Mais facilidade no repassamento dos resultados para os alunos;
- O treinamento não fica mais preso à necessidade de formação de turmas ou grupos;

Quando se tem um curso a distância normalmente a avaliação não é feita da mesma forma, o que gera para o avaliado, em muitos casos, custos de transporte, hospedagem que poderiam ser evitados se houvesse uma avaliação no seu local de domicílio. No entanto, a instituição, tendo que aplicar a avaliação no local de domicílio do avaliado, passa a ter custos relacionados:

- A Logística:
  - Empacotamento e transporte da avaliação ;
  - Segurança do transporte da avaliação ;
  - Mão de obra para segurança e auditoria da lisura do processo;
  - Hospedagem e transporte da mão de obra ;
  - Aluguel de espaço para a avaliação ;
- A impressão de material ;
- Eliminação da necessidade de manter ou alugar salas de aula ;
- Diminuição da velocidade do processo.

Faz-se assim a necessidade da criação de grupos para aplicação da avaliação. Desta forma observa-se que a não aplicação de avaliação a distância faz com que haja uma redução no ganho que se pode ter no uso de ensino a distância com uso de Internet.

3.7 Processo de Ensino a Distância

Autores como [DRI 98, GIU 00] apontam modelos a serem seguidos para a implantação de um programa de ensino a distância e consideram que a última etapa de um programa de ensino deve ser a Avaliação e medição da transferência de conhecimento. Fica claro em [VAS 98], que a existência desta etapa não impede que se aplique avaliações esporádicas que devem ser usadas para acompanhar o desenvolvimento do treinando durante todo o processo com o objetivo de servir de base para melhoria do material.

3.8 Conclusão

Lorrainne Sherry, em [SHE 96], afirma que, ”sem conectividade, o ensino a distância degenera no antigo modelo de cursos por correspondência. O estudante torna-se autônomo e isolado, procrastinado, e eventualmente desiste.” Pode-se, sem sombra de dúvidas, afirmar que neste processo interativo é extremamente importante a existência de mecanismos que permitam avaliar o desempenho do estudante e gerem informações que sirvam de base para melhoria do curso. Jacobsen, [JAC 94], apresenta que do ponto de vista institucional a tecnologia é considerada uma importante geradora de expectativas, quanto a criação e disponibilização de novos serviços que forneçam maior efetividade e menores custos que a construção de novos campus. O uso de um software que permita avaliação a distância pode ser extremamente útil para a concretização desta visão das instituições.

Capítulo 4

Análise dos Sistemas Disponíveis

4.1 Introdução

A avaliação na educação à distância é uma das ferramentas que o professor possui para conhecer o aluno e refletir sobre como melhorar o curso ou orientar o aluno. As avaliações devem ser realizadas de forma a não suscitar dúvidas sobre sua validade. Apresenta-se aqui o caso da empresa Prometric, na seção 4.2 e a visão geral de um trabalho que possui em seu objetivo características semelhantes a esta dissertação, na seção 4.3.

4.2 Prometric

O “software” usado no processo de certificação da Prometric, conforme detalhado em 2.4.2 , não se aplica a um modelo não presencial, pois ele requer o deslocamento para uma unidade certificadora. O “software”, por ser proprietário, não tem sua especificação publicada, portanto não se pode determinar, por exemplo, que a avaliação esteve privada para todos os candidatos até o momento da avaliação, segundo a Prometric a avaliação é arquivada em seus computadores e das suas coligadas ou filiais de forma segura (*cifrada*) e a transmisão é feita através de um canal seguro com uso de técnicas de criptografia, no entanto o algoritmo usado no processo não esta especificado

na documentação liberada. Desta forma observa-se que o princípio de *Kerckhoff*, visto em 5.2, não é adotado pela Prometric.

A não repudiação é fornecida pela assinatura de um documento que comprova o comparecimento na unidade certificadora e a autenticação pela conferência da identidade do avaliado feita pelo administrador do centro autorizado de avaliação. O sistema fornece meios para que o candidato possa contestar a avaliação mas estes não são detalhados. O avaliado não possui como determinar se a avaliação foi alterada antes da sua aplicação ou após, não sendo assim possível verificar a integridade.

O certificado emitido não possui uma identificação digital, e todos os itens de segurança, com exceção da assinatura do responsável pelo sistema, são de fácil adulteração ou reprodução.

4.3 Autenticação para Usuários no Ensino a Distância

O SBRC 2000 publicou o trabalho de [FIO 00] que procura solucionar problemas relacionados à autenticação de usuários em softwares de ensino à distância, o trabalho foca na criação de um protocolo que permite a identificação dos usuários durante toda a sessão de treinamento, procurando desta forma garantir que o avaliado é quem realmente alega ser durante a avaliação.

4.3.1 Autenticação

Em seu trabalho [FIO 00] produziu um módulo que integra diferentes soluções de autenticação onde as diversas soluções tecnólogicas são empregadas em conjunto conforme apresentado na lista a seguir:

- **Senha**: O usuário para acessar a avaliação deve fornecer uma senha o sistema o resumo (*hash*) desta calculado pelo algoritmo *MD5* e compara este valor com o resumo que está armazenado em um banco de dados, esta solução impede que o administrador tenha acesso a senha do usuário;

- **Perguntas randômicas**: durante a sessão são feitas perguntas ao usuário baseadas em dados pessoais previamente armazenados, criando-se desta forma uma espécie de desafio. O sistema é capaz ainda de fazer perguntas baseando-se no histórico de uso do sistema;

- **Dispositivos biométricos**: randomicamente pode ser acionado um dispositivo para autenticação biométrica como câmeras para identificação da face.

O acesso ao sistema dá-se após o aluno iniciar a aplicação que irá permitir a realização do *login*. Neste momento lhe serão requisitados os dados de autenticação (nome, senha e/ou extração do dado biométrico). Estes dados serão enviados para o módulo de autenticação, que verificará se são válidos. Se os dados forem válidos, o sistema buscará na base de dados uma pergunta pessoal aleatória e desafiará o usuário. Se ele responder corretamente à pergunta, estará autenticado no sistema, e lhe será apresentada a página inicial com os cursos em que está matriculado. Uma resposta ou dado inválido, em qualquer etapa deste processo, negará o acesso do aluno ao sistema. Nota-se que a senha não trafega pela internet apenas o Hash desta calculado pelo algoritmo MD5, no entanto como o sistema usa este valor para autenticar o usuário um escuta que roubar este valor pode obter um acesso prévio ao sistema se passar por uma pessoa autorizada até que um dos outros dispositivos entrem em ação conforme figura 4.1, este problema deixado no trabalho é facilmente resolvido com a adoção de um protocolo que garanta a segurança do canal como, por exemplo, *Secure Socket Layer* (*TLS*).

As alternativas para autenticação e monitoramento são válidas e funcionais fica claro no trabalho de Fiorese que não existe a intenção de fornecer 100% de garantia quanto a segurança no acesso e uso.

4.3.2 Privacidade

Em nenhum momento o trabalho usa mecanismos que dificultem ou impeçam escutas das comunicações feitas entre a instituição de ensino e o treinando ou avaliado. Umas solução simples para este problema seria a criação de um canal seguro com o uso do protocolo *TLS*.

4.3.3 Integridade

Não são fornecidos no trabalho mecanismos que permitam a verificação da integridade das páginas acessadas pelos usuários do sistema. As provas e questões poderiam receber uma assinatura digital verificável pelo avaliado.

4.3.3.1 Não Repudiação

Não é fornecida nenhuma característica que possa garantir a não repudiação. A assinatura eletrônica do avaliado nas avaliações e para cada avaliação entregue a emissão de recibo por parte do avaliador resolvem o problema da não repudiação. A instituição possui assim um documento com a assinatura do avaliado e o avaliado possui um documento com a assinatura do avaliador, estes documentos podem ser usados no caso de disputas ou dúvidas sobre a realização da avaliação.

4.4 Conclusão

[LAU 01] observa o seguinte:

> ”Quando se trata de contratos celebrados eletronicamente, deve-se concordar que não é fácil identificar quem realmente se encontra por trás do monitor de um computador”

Neste complexo problema é onde [FIO 00] se concentra deixando de lado todos os outros que podem vir a ocorrer durante o processo de avaliação à distância. Deixando assim uma lacuna a ser preenchida quanto aos quesitos de:

- Segurança no canal;
- Integridade dos documentos;
- Garantia de não repudiação.

Esta dissertação concentra-se nos itens acima que não são explorados por [FIO 00] e deixa de lado o processo de autenticação que é amplamente discutido e

tratado por este, o protocolo aqui proposto pode perfeitamente vir a ser no futuro único ao trabalho de Fiorese.

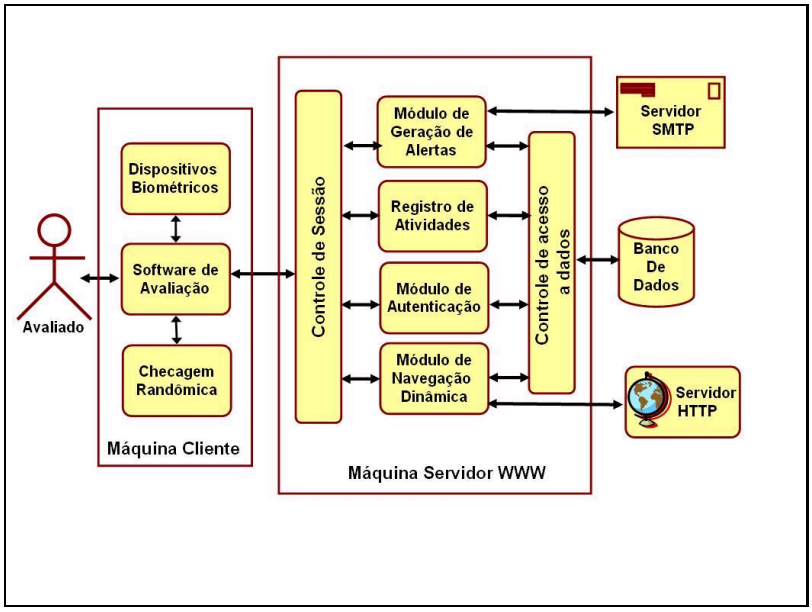

Figura 4.1: Autenticação de usuários: A proposta de [FIO 00] funciona como uma espécie de intermediário, em inglês *proxy*, entre o servidor *Web* e o avaliado. Este intermediáro tem por objetivo controlar o acesso à páginas através da combinação de senhas, perguntas randômicas dinâmicas, dispositivos biométricos e checagem randômica, ao mesmo tempo que registra as atividades, ou seja, gera *logs*. Os registros conterão informações como dia e hora do acesso, tempo dispendido em cada página, endereço *IP* da máquina que realizou o acesso, entre outras informações. As informações recolhidas podem ser usadas em um curso para avaliar o aluno e também para gerar seu perfil estatístico. O perfil servirá para gerar alertas na medida em que ocorrerem,durante a atividade do aluno, mudanças de hábitos acima dos limites estabelecidos. Para que apenas pessoas autorizadas possam acessar s páginas, as mesmas são geradas dinamicamente.

Capítulo 5

Segurança

5.1 Introdução

Com a grande proliferação de computadores e sistemas de comunicação que se iniciou na década 1960 houve uma grande demanda por parte do setor privado de meios para proteger informações digitais e de prover segurança para serviços computadorizados [MEN 96], tornando-se assim extremamente necessária a definição de Protocolos de Segurança, os quais descrevem uma seqüência de interações seguidas durante a comunicação entre entidades para garantir que ocorra no processo o alcance de objetivos como [SCH 01, BER 98]:

- Confidencialidade;
- Integridade;
- Anonimato;
- Não-repudiação.

Estes objetivos são atingidos através da aplicação dos protocolos que tipicamente empregam nos seus passos técnicas criptográficas e envolve a troca de termos de um contrato com a intenção de estabelecer um acordo entre partes que podem possuir interesses conflitantes. Ressalta-se a existência de características como [BER 98]:

- São baseados em uma série de passos, ou seja, possuem uma seqüência de execução onde:
  - cada passo deve ser executado para permitir a execução do próximo;
  - nenhum passo pode ser executado antes de finalizado o passo anterior;
  - ao menos duas pessoas são necessárias para executar um protocolo;
- Todos envolvidos no protocolo devem conhecer os passos antecipadamente;
- Todos envolvidos devem concordar com o protocolo;
- O protocolo não pode ser ambíguo, todos os passos devem ser bem definidos;
- O protocolo deve ser completo, ou seja, deve existir uma ação específica para cada possível situação;

As principais dificuldades para projetar um protocolo de comunicação que garanta segurança são apontadas a seguir [SCH 01]:

- As propriedade que supostamente um protocolo deve garantir são muitas vezes difíceis de detectar;
- Protocolos normalmente são executados em ambientes complexos e hostis. Para avaliar o protocolo muitas vezes é necessário descrever e detalhar acuradamente o ambiente.
- Pode ser extremamente difícil detalhar as capacidade dos agentes hostis. Os agentes hostis são muitas vezes encontradas ou especificados na literatura como: intrusos, espiões, inimigos, atacantes. Neste trabalho os agentes hostis e os demais envolvidos serão denominados participantes.

Este capítulo apresenta um visão geral das técnicas de criptografia que são aplicadas para prover segurança em protocolos e prover a base de conhecimentos necessárias para avaliar a segurança dos sistemas disponíveis apresentados no capítulo 4. As técnicas apresentadas permitem a definição do protocolo apresentado no capítulo 6.

5.2 Criptografia

Cifrar é o processo de transformar dados, denominados texto aberto, para um formato no qual seja impossível sua leitura (texto cifrado) sem a posse de algum conhecimento, como, por exemplo, uma chave [ROG 95]. Decifrar é o processo reverso de cifrar; é a transformação de um texto cifrado em texto aberto. O uso da criptografia permite desta forma a comunicação segura em um ambiente hostil [ROG 95], O documento cifrado pode assim ser usado para compartilhar informações sigilosas de maneira segura mesmo na presença de adversários. Pode-se, portanto, dizer-se que criptografia diz respeito a manter segredo em comunicações (cifrar), entretanto, esta é apenas uma parte do uso da criptografia atualmente. No entanto, de maneira mais formal [MEN 96],

> Estudo de técnicas matemáticas relacionadas aos aspectos de segurança da informação como confidencialidade, integridade de dados, autenticação das entidades, confirmação da origem.

A criptoanálise é a ação de tentar descobrir a mensagem ou a chave [STA 99]. Os algoritmos aqui apresentados baseiam-se no amplamente aceito e adotado [STA 99, BER 98, MEN 96, NEW 97] princípio de *Kerckhoff*:

- A segurança de um sistema criptográfico não deve depender de se manter segredo do algoritmo usado no sistema. Deve ser dependente somente de se manter segredo da chave usada.

.

5.2.1 Criptografia Simétrica

O algoritmo de cifragem, também conhecido por cifrador, a partir da chave transforma o texto aberto em texto cifrado, com base em substituições, permutações ou funções matemáticas. O texto cifrado é dependente do texto aberto e da chave, o texto aberto e a chave são independentes entre si.

Define-se um criptossistema como sendo $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ tal que:

- $\mathcal{P}$ um conjunto finito de possíveis textos planos;
- $\mathcal{C}$ um conjunto finito de possíveis textos cifrados;
- $\mathcal{K}$ espaço de chaves, um conjunto finito de chaves possíveis;
- para cada $\mathcal{K}$, há uma regra de cifragem $\in \mathcal{C}$ e uma regra de decifragem correspondente $\mathcal{D}$. Cada $\mathcal{P} \rightarrow \mathcal{C}$ e d_K são funções tais que $d_K(e_K(c)) = p$ para cada texto aberto $\in \mathcal{P}$.

Os algoritmos criptográficos usados hoje em dia foram fortemente influenciados pelo trabalho de *Horst Feistel* na *IBM* no início de 1970, publicado em [AME 73], e culminando em 1977 com a adoção de um protocolo padrão de criptografia para uso em comunicações em órgãos do governo Norte Americano, DES. São exemplos de cifradores simétricos os algoritmos *DES, Blowfish, IDEA, CAST e RC5* [STA 99].

5.2.2 Criptografia Assimétrica

Até 1976 a única forma de criptografia existente era a criptografia simétrica, que foi afetada durante toda sua história pelo problema de como estabelecer um canal seguro para a transmissão da chave para todas pessoas que necessitam, pois se a chave cair nas mãos do inimigo ela deixa de cumprir sua tarefa [NEW 97]. Os sistemas de criptografia assimétrica também são conhecidos por criptografia de chave pública. A idéia por trás de um sistema de chave pública é considerada por [MEN 96] como a mais importante criação na história da criptografia tendo surgido do trabalho de Diffie e Hellman [STA 99] após a publicação do artigo "New Directions in Cryptography" [MEN 96]. O trabalho de Diffie e Hellman propõe um sistema criptográfico em que [STA 99]:

- Computacionalmente fácil gerar um par de chaves (*chave pública* KU_b, *chave privada* KR_b);
- Computacionalmente fácil para um transmissor a, conhecendo a chave pública do receptor b e a mensagem a ser cifrada, M, gerar o texto cifrado correspondente;

Tabela 5.1: Aplicação dos Algoritmos Assimétricos. A tabela demonstra que o algoritmo que será adotado em um protocolo depende diretamente dos serviços que serão necessários no protocolo.

Algoritmo	**Cifrar e Decifrar**	**Assinatura Digital**	**Troca chave**
RSA	SIM	SIM	SIM
Diffie-Hellman	NÃO	NÃO	SIM
DSA	NÃO	SIM	NÃO

- $C = E_{KU_b}(M)$;
- Deve ser computacionalmente fácil para o receptor B decifrar o texto usando a chave privada para recuperar a original:
- $M = E_{KU_b}[D_{KR_b}(M)]$
- Computacionalmente impossível para um oponente, conhecendo a *chave pública*, KU_b, descobrir a *chave privada*, KR_b.
- Computacionalmente impossível para um oponente, conhecendo a *chave pública*, KU_b, e uma mensagem criptografada, (C), para recuperar a mensagem original.

Pode-se adicionar um sexto requisito que, embora útil, não é necessário para todas as aplicações de chave pública:

- As funções de cifragem e decifragem podem ser aplicadas em uma ou outra sequência: $M = E_{Ku_b}[D_{KR_b}(M)]$

A tabela 5.1 apresenta exemplo de alguns algoritmos assimétricos e seu respectivo uso.

5.2.3 Sistemas Criptográficos Híbridos

Algoritmos assimétricos não substituíram os algoritmos simétricos. As duas técnicas são normalmente adotadas em conjunto, onde os algoritmos assimétricos

servem para cifrar chaves privadas que são adotadas para cifrar as mensagens. Esta técnica é adotada pois os algoritmos assimétricos são, conforme [BER 98], considerados:

- lentos, comumente numa razão de 1 para 1000 comparando-se com os simétricos
- vulneráveis ataque texto original escolhido.

Algoritmos assimétricos são normalmente adotados para transmitir de forma segura chaves de sessão que são usadas para cifrar mensagens garantindo o sigilo e a autencidade das comunicações conforme [SCH 98] que são normalmente executadas em sessões como a seguir [SCH 98, ROG 95]:

1. Beto envia sua chave pública para Alice;
2. Alice gera randomicamente uma chave de sessão, k;
3. Alice cifra a chave de sessão e envia para Beto $E_{KU_b}(k)$;
4. Beto decifra a chave de sessão de Alice usando sua chave privada $D_{KR_b}(k) = K$;
5. Alice e Beto podem agora comunicar-se usando a chave de sessão;

5.2.4 Função Resumo

A função de caminho único também denominada resumo ou função *Hash*, transforma uma entrada de tamanho variável, no caso mensagens de qualquer tamanho, numa saída de tamanho fixo, a função garante que, se a informação é mudada, até mesmo uma única letra, uma saída completamente diferente será produzida. Esta saída é também conhecida por "message digest" e pode ser entendida como a essência da informação. Ela traduz todo o conteúdo de um texto para uma seqüencia de caracteres de tamanho fixo. Define-se uma função como sendo de caminho único quando para a função h que produz o resumo z for computacionalmente inviável encontrar uma mensagem x, tal que $h(x) = z$. Resumos são usados comumente para garantir a integridade de informações baixadas pela *Internet*. Pode-se, por exemplo, para cada arquivo

disponibilizado em um servidor, disponibilizar um resumo. O usuário que baixar o arquivo poderá calcular o resumo do arquivo baixado e comparar o valor resultante como resumo disponibilizado, se form iguais, significa que o arquivo baixado está íntegro, caso contrário deve-se desconfiar da integridade do arquivo baixado, pois existe a possibilidade do resumo estar errado.

Uma outra aplicac ao para as func oes de resumo seria por exemplo, garantir a integridade das informac oes obtidas atraves de um download. Um arquivo baixado pela Internet com o seu respectivo resumo concatenado. Apos isso, calcula-se o resumo da mensagem original e compara-se com o recebido. Se forem iguais, o download sucesso e a integridade dos dados est garantida.

5.2.5 Sistemas de Autenticação

O uso de criptografia possibilita a resolução de problemas aparentemente impossíveis de serem resolvidos [STI 95]. Como permitir autenticação, ou seja, duas ou mais pessoas tornam-se capazes de se identificar e reconhecer mutuamente sem possibilidade de engano [BOL 96]. Garante-se desta forma que em um determinado protocolo Beto seja capaz de reconhecer Alice e vice-versa e que Mallory jamais conseguirá se passar por Beto e enganar Alice, ou conseguirá fingir que é Alice.

No cotidiano existem muitas situações onde é necessário "provar" eletronicamente a identidade de alguém [STI 95].

5.2.5.1 Identificação com Algoritmos Híbridos

Um modelo simples de identificação é proposto por [STI 95] baseado no uso de técnicas de criptografia simétrica, como o *DES*. O protocolo, descrito a seguir, é denominado protocolo de desafio-e-resposta.

- Beto escolhe um desafio, x, que é uma cadeia de caracteres randômica de 64 posições;
- Beto envia x à Alice;

- Alice calcula $y = eK(x)$;
- E o envia para Beto;
- Beto calcula $y' = eK(x)$;
- E verifica que $y' = y$.

O autor explica que assumindo que Alice e Beto usem uma função criptográfica que faz uso de um expoente modular como $eK(x) = x^{101379} \ mod 167653$ e supondo que o desafio de Beto é x =77835. Então Alice responde com y = 100369. O protocolo funciona, pois Alice e Beto possuem um segredo compartilhado. Como exemplos de autenticação com criptografia simétrica pode-se citar [SCH 98] SKID, Wide-Mouth Frog, Yahalom, Needham-Schroeder, Kerberos, Otway-Rees onde a maior parte destes faz uso de uma entidade confiável para garantir a segurança do protocolo. O protocolo Needham-Schroeder [SCH 98] por possuir falhas de segurança sofreu alterações por parte dos seus autores após publicação e acabou se tornando muito semelhante ao protocolo Otway-Rees [SCH 98].

5.2.5.2 Identificação com Algoritmos Assimétricos

Alice e Beto podem usar criptografia híbrida para determinar uma chave de sessão, e usar esta para cifrar dados como visto anteriormente em 5.2.3. Sendo este protocolo extremamente simples de ser construído. Este protocolo é suscetível no entanto ao ataque *Man-in-the-middle* caso as chaves públicas de Beto e Alice não sejam assinadas ,detalhado em 5.2.6), por uma entidade certificadora, detalhado em 5.2.8, por exemplo. Usando algoritmos assimétricos [STA 99] tem-se os protocolos DASS, Denning-Sacco, Woo-Lam.

5.2.6 Assinatura Digital

Uma das mais importantes contribuições da criptografia assimétrica é a possibilidade de assinarmos documentos digitais. Uma assinatura deve possuir por características [LAU 01, BER 98, STA 99, STI 95]:

1. Confiável, ou seja, permite verificar a autenticidade da assinatura;

2. Não é falsificável: somente o proprietário da assinatura pode produzí-la;

3. Não é reutilizável: não existe forma de pegar uma assinatura recebida e usar em outra mensagem;

4. Não é repudiável: a pessoa que assinou não possui mecanismos para negar que assinou o documento;

5. Preserva a integridade do documento: após o documento. ter sido assinado ele não pode ser alterado

5.2.6.1 Definição Formal

Um esquema de assinatura consiste de dois algoritmos públicos sendo um para realizar a assinatura e outro para verificação. O algoritmo de verificação retorna "*verdadeiro*" ou "*falso*" de acordo com a autenticidade da assinatura. Formalmente um esquema de assinatura digital é uma quintúpla (P, A, K, S, V) onde as seguintes condições são satisfeitas [STI 95]:

1. P é um conjunto finito de possíveis mensagens;

2. A é um conjunto finito de possíveis assinaturas;

3. K, espaço de chaves, é um conjunto finito de possíveis chaves;

4. Para cada K ϵK, existe um algoritmo de assinatura $ver_K \epsilon S$ e um algoritmo de verificação correspondente $ver_K \epsilon V$. Cada $sig_K :\rightarrow A$ e $ver_K : P \times A \rightarrow \{verdadeiro, falso\}$ são funções de tal forma que as equações são satisfeitas para cada mensagem $x \epsilon P$ e para cada assinatura $y \epsilon A$:

$$ver(x, y) = \begin{cases} verdadeiro & se\ y = sig(x) \\ falso & se\ y \neq sig(x) \end{cases}$$

Para cada K ϵK as funções ver_K e $sign_K$ devem ter tempo de processamento polinomial, tornando assim o processo computacionalmente seguro.

Assinatura digital pode ser obtida por meio da criptografia de um resumo da mensagem denominada função de condensação ou função de caminho único, aqui sendo simbolizado pela função *H()*, com a chave privada da entidade que está assinando a mensagem: $S_A(M) = E_{KR_A}(H(M))$ conforme [STA 99].

5.2.6.2 Algoritmos Para Assinatura

Em 1991 o primeiro padrão internacional de assinatura digital foi definido (ISO/IEC 9796). O padrão baseia-se no algoritmo de chave pública do RSA. No ano de 1994, o Governo Americano definiu o seu padrão de assinatura digital como sendo o Digital Signature Standart (DSS) baseado no mecanismo de chave pública ElGamal, o padrão faz uso do Secure Hash Algorithm (SHA). O DSS foi proposto pelo Instituto Nacional de Padrões e Tecnologia (NIST - USA). A proposta original foi feita em 1991 e foi revisado duas vezes (1993 e 1996) [STA 99].

O algoritmo foi projetado para oferecer somente assinatura digital, não podendo ser usado para criptografia ou troca de chave. Pode-se descrever o funcionamento do algoritmo pelos seguintes passos:

- O resumo da mensagem é calculado;
- Um número randômico k é gerado para esta assinatura;
- O resumo da mensagem mais um número randômico são fornecidos como entrada para a função de assinatura.

Como exemplos de algoritmos de assinatura digital, pode-se citar o DSS [STA 99] e o RSA [STA 99].

5.2.6.3 Assinatura em Arquivos Longos

Assinaturas digitais são extremamente ineficiente quando aplicadas a arquivos grandes [STI 95] nota que a aplicação do DSS 6 permite apenas a assinatura de

”*pequenas*” mensagens e que sua aplicação em uma mensagem de 160 bits por exemplo resulta em uma assinatura de 320 bits. Como uma possível solução para este problema pode-se dividir mensagens maiores em blocos de 160 bits e assinar cada um dos blocos, no entanto esta hipótese é inviável devido ao fato de que a mensagem dobra de tamanho quando somada a assinatura e tem-se ainda o problema da baixa velocidade para a assinatura de documentos. Uma técnica eficaz e amplamente adotada para assinar arquivos longos consiste em gerar para o arquivo de um resumo (*hash*) e assinar este resumo.

5.2.6.4 Assinatura às Cegas

Pode-se desejar em um protocolo que um dos participantes assine e - ateste a autenticidade de um documento sem ver seu conteúdo, no mundo real pode-se adotar a estratégia apresentada por Schneier em [SCH 98] onde o documento que deve ser assinado é colocado junto com um papel-carbono dentro de um envelope para assinar cegamente o documento basta agora assinar o envelope e a assinatura será transferida para o documento. Tipicamente assinaturas cegas são adotadas para provar que um documento existia em um determinado momento no tempo. Em [SCH 98], encontra-se um exemplo simples de assinatura cega:

1. Alice multiplica o conteúdo do documento por um valor randômico, este valor é denominado fator de ocultação ;
2. Alice envia o documento que resultou da multiplicação para Beto;
3. Beto assina o documento;
4. Alice armazena para comprovação futura o fator de ocultação e o documento original;

O exemplo apresentado funciona para os casos em que a assinatura e o fator de ocultação são comutativos, em caso negativo existem outras operações que podem ser efetuadas.

David Chaum, de acordo com [SCH 98], inventou usando RSA o conceito de assinatura cega. A implementação mais simples considera que Beto possui uma

chave publica, e, e uma chave privada , d e um módulo público, n. Para que Beto assine cegamente uma mensagem qualquer de Alice representada por m é necessário:

1. Alice escolhe um valor randômico denominado k que se encontre entre 1 e n;
2. Alice oculta m calculando: $t = mk^e \ mod \ n$
3. Beto assina t com : $t^d = (mk^e)^d \ mod \ n$
4. Alice desoculta t^d calculando: $s = \frac{t^d}{k \ mod \ n}$
5. O que resulta em $s \equiv m^d mod n$ que é demonstrado por $t^d \equiv (mk^e)^d \equiv m^d k (mod n)$ então $\frac{t^d}{k} = \frac{(m^d k)}{k} \equiv m^d (mod \ \ n)$;

A complexidade de uma assinatura cega é igual à de uma assinatura digital comum, conseqüentemente, assinaturas cegas são geralmente a forma mais aceita de se obter anonimato, de acordo com [DEV 01].

5.2.7 Datação Digital

Assinaturas digitais garantem que a informacão contida em um documento não pode ser modificada sem que se detecte a mudança. De acordo com [PAS 02][1], para que a assinatura digital tenha validade jurídica, além de associar o conteúdo de um documento a uma pessoa, este deve ser associado também a uma posição no tempo, data e hora, de quando o documento foi assinado. A datação digital tem como objetivo assegurar a existência de um documento eletrônico qualquer em uma determinada data e hora. Diversos sistemas de datação baseiam-se no uso de uma entidade confiável chamada de Autoridade de Datacão - PDDE (*Time-Stamping Authority*). Uma PDDE é responsável em disponibilizar um serviço de datação confiável e de acordo com a legislação do pais em que atua.

A PDDE recebe um documento, ou resumo (*hash*), e acrescenta data e hora no documento, armazena uma cópia que pode ser usada em caso de disputa e devolve

[1]O trabalho de [PAS 02] traz maiores informações sobre o processo de datação digital e sobre as empresas que realizam este serviço.

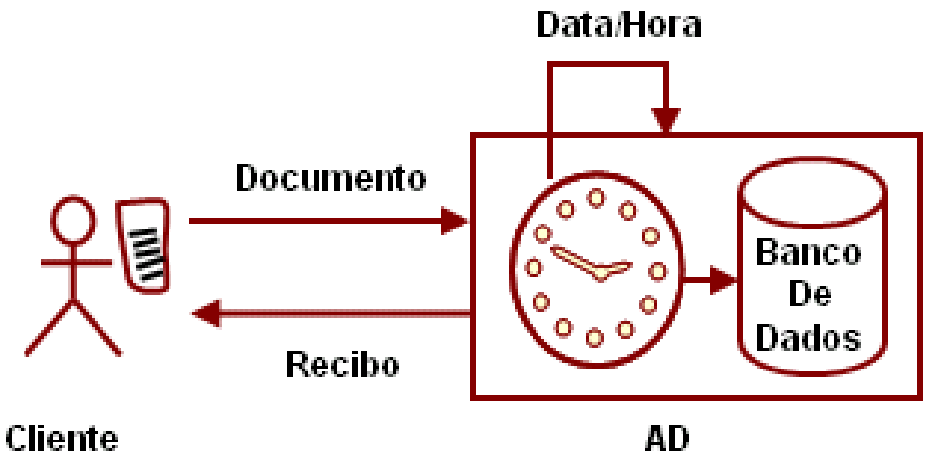

Figura 5.1: Processo de datação. O cliente envia para uma datadora (PDDE) o documento para ser datado. A PDDE por sua vez anexa data e hora ao documento, armazena um cópia em seu banco de dados e remete um recibo assinado para o cliente.

um recibo assinado indicando que o documento foi datado, de forma resumida o processo pode ser visto na figura 5.1. A partir de um convênio com a Universidade Federal de Santa Catarina, a BRy Tecnologia (*http:/www.bry.com.br*), desenvolveu uma solução nacional de PDDE.

5.2.8 Certificado Digital

Em um ambiente de chave pública, é vital a garantia de que a chave pública que está em uso é de fato a chave do usuário desejado e não uma falsificação. Poderia-se simplesmente cifrar dados para chaves de pessoas para as quais a chave foi recebida de forma pessoal. Mas supondo-se que se queira trocar informações com alguém que se conheceu, por exemplo, na *Internet*. Torna-se problemático garantir a posse da chave correta. Um certificado é uma forma de credencial. Exemplos disso são o Registro Geral (*RG*), o *CPF*. e a Carteira de Habilitação. Cada um deles tem alguma informação identificando a pessoa de alguma forma e são todos emitidos por autoridades

que garantem a validade do documento, no caso dos documentos acima citados, é feito pelos órgãos públicos. Um certificado digital contém dados que funcionam como um certificado físico. Nele está contido a informação referente à pessoa, à sua chave pública e outras informações que permitam aos outros verificarem se a informação contida no certificado é genuína ou não. Certificados digitais são usados para impedir a substituição de uma chave pessoal por outra, sendo em muitos casos emitidos por autoridades neste caso denominadas de Autoridade Certificadora, em inglês CA. Um certificado Digital basicamente consiste de:

- Uma chave pública;
- Informações que identificam o dono (nome, número de identificação, estado ,etc.);
- Uma ou mais assinaturas digitais;
- O período que o Certificado é válido.

O objetivo da assinatura digital no certificado indica que uma outra entidade (a autoridade certificadora) garante a veracidade das informações nele contidas. A assinatura digital não atesta a autenticidade do certificado como um todo, ela se responsabiliza apenas em garantir que a informação contida no certificado está ligada a chave pública, impedindo a substituição ilegal de informações ou da própria chave. Um certificado é basicamente uma chave pública com uma ou duas formas de identificação anexadas, mais uma impressão central de confiança, garantindo a identidade do indivíduo. O certificado X.509 v3 é um padrão popular para certificados de chave pública, sendo este padrão amplamente usado por muitos protocolos modernos de criptografia, inclusive o TLS que permite acesso seguro a sites na Internet. Cada certificado X.509 contém um número de versão, um número serial, informações de identidade, informações relacionadas ao algoritmo e a assinatura do órgão emissor. A indústria adotou os certificados X.509 v3 (no lugar das versões anteriores) porque eles permitem a inserção de dados arbitrários no certificado, que podem ser utilizados para propósitos variados. O certificado tem um período de tempo limitado quando ele é válido. Ele identifica o nome da organização e o país no certificado; o nome da organização emissora da assinatura; o

algoritmo que foi usado na assinatura; a chave pública; e por último, a assinatura do certificado. Em [STA 99] é mostrado detalhadamente a estrutura de dados e o formato dos campos utilizados para cada uma.

5.3 Conclusão

Protocolos de segurança, que empregam criptografia, podem ser usados para garantir o fluxo normal das comunicações evitando problemas como os apresentados por [STA 99] que são listados a seguir:

- Interrupção;
- Modificação;
- Intercepção;
- Fabricação.

A criptografia pode ser útil ainda na autenticação das partes e documentos no processo de comunicação. A definição de uma proposta de um protocolo para *Segurança na Avaliação não Presencial* necessita de diversos conhecimentos na área de criptografia como conceitos de: criptografia assimétrica, criptografia simétrica funções resumo, assinatura digital, certificado digital e infra-estrutura de chave pública. O simples uso destes fundamentos não garantem por si só segurança sendo necessário definir a seqüência de passos a serem executados, o que é feito no capítulo 6.

Capítulo 6

Descrição do Modelo

6.1 Introdução

O protocolo de avaliação a distância, proposto neste capítulo, visa - fornecer segurança e validade jurídica dos documentos. Ou seja, garantir a validade, autenticidade e integridade dos documentos quando avaliador e avaliados encontrarem-se separados no espaço, usando uma rede como canal de comunicação, conforme definido no objetivo geral apresentado na subseção 1.1.1. Os conhecimentos sobre o processo de avaliação, resumidos nos capítulos 2 e 3 e unidos às tecnologias de segurança que foram previamente apresentadas no capítulo 5 e 4, permitem a definição deste protocolo.

Unificam-se, neste capítulo, os processos adotados nas *competições* e nas *avaliações do conhecimento*. Estes dois modelos estão definidos na subseção 1.1.3 e decompostos e analisados no Capítulo 2, que revela a existência de pequenas diferenças entre os dois modelos quanto aos objetivos, grau de formalidade, exigência por segurança. A definição de um protocolo que atenda as duas é possível pelo fato de ambos possuírem as mesmas atividades, pode-se dizer que *competições* tendem a ser executados com regras de segurança mais rígida.

6.2 Requisitos de Segurança

A garantia de segurança passa pela definição de princípios que norteiem a definição do protocolo. Ou seja, é necessário, antes de definir o protocolo determinar os objetivos a serem atingidos. Aceitam-se aqui por válidos e aplicáveis os princípios legais, que foram detalhados anteriormente na subseção 2.2. Do ponto de vista computacional, para garantir os princípios legais adota-se um conjunto de requisitos de segurança, descritos a seguir:

- **Igualdade e impessoalidade** - Todos avaliados durante todo o processo de avaliação do conhecimento serão tratados de forma idêntica, pelo protocolo. Garante-se assim a validade e o cumprimento da finalidade da avaliação.

- **Publicidade** - Os resultados, o protocolo e os programas usados[1]no processo devem ser públicos. Garante-se assim transparência ao processo de avaliação.

- **Verificabilidade** - Avaliado ou avaliador, caso achem necessário, devem poder verificar uma ou mais avaliações manualmente. Os resultados, o protocolo e os programas usados no processo devem ser públicos.

- **Confidencialidade** - Apenas os participantes de uma determinada comunicação podem ter conhecimento do conteúdo das mensagens trocadas.

- **Integridade** - As mensagens enviadas em uma comunicação serão transmitidas de forma fiel, ou seja, não serão alteradas durante o caminho.

- **Correta autenticação** - Fornece garantia da identidade dos participantes de uma comunicação. Ou seja, deve impedir que uma pessoa assuma a identidade de outra.

- **Não recusa** - Fornece garantia de que o emissor não pode no futuro negar a autoria de uma mensagem.

[1]Os programas devem ser assinados digitalmente e os interessados em verificar o código são liberados a usar técnicas de engenharia reversa. Opcionalmente pode-se eleger auditores que periodicamente verificam e atestam os programas, porém esta decisão cabe a instituição e não faz parte do protocolo.

6.3 Atividades do Processo

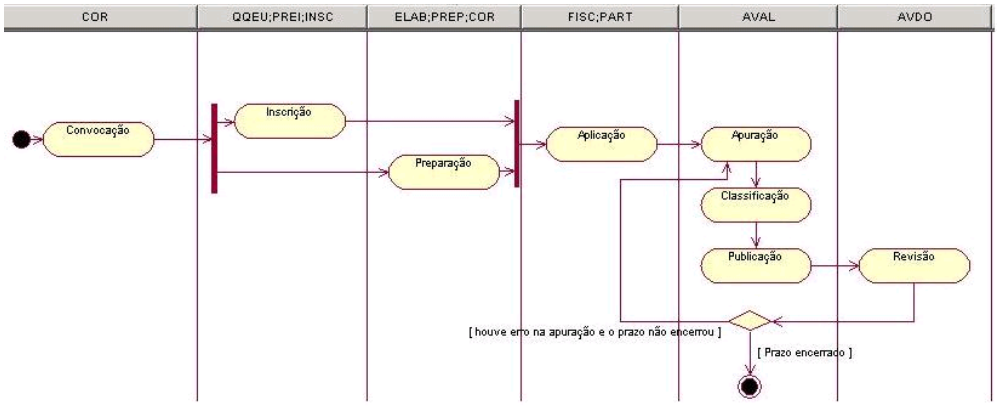

Figura 6.1: Funcionamento do processo de avaliação. Pelo diagrama pode-se observar em quais atividades os usuários participam e que atividades de inscrição e preparação podem ser executadas em paralelo.

O processo de avaliação possui as mesmas atividades em todos os - modelos de avaliações, conforme percebe-se pela leitura da apresentação realizada em 2 (Aplicação de avaliações) e 3 sobre o processo de aplicação de avaliações, sejam elas *competições* ou *avaliações do conhecimento*. Sendo assim, pode-se detalhar o processo de avaliação como sendo a execução das atividades, previamente definidas por [FIL 01]: convocação e divulgação; preparação; inscrição; aplicação; apuração; classificação; publicação; revisão e divulgação.

As atividades enumeradas são executadas seqüencialmente, de acordo com [FIL 01]. Extrapola-se aqui esta proposta ao se adotar o modelo da Figura 6.1, onde a atividade de preparação pode ser executada em paralelo com a atividade de inscrição.

6.4 Identificação dos Participantes

De acordo com [SCH 01, AND 96] uma das principais armadilhas na especificação de um protocolo é a incapacidade do projetista de identificar e modelar as

necessidades de todos participantes. Para evitar esta armadilha, os participantes foram detalhados usando a união das técnicas descritas por [WIN 98] com técnicas *Unified Modeling Language* (*UML*) [JAC 95, JAC 98, PJ 01, QUA 98]. Por isto, [AND 96], aponta que na definição de um protocolo a primeira preocupação do projetista é encontrar os participantes que de modo genérico são listados através do nome dos seus papéis. Os seguintes tipos de participantes foram identificados :

- **AUSE - Ausente**: aquele que está inscrito, mas não participa da avaliação;
- **AVAL - Avaliador**: aquele que analisa e determina o valor das avaliações;
- **AVDO - Avaliado**: aquele a que se deu valor determinado;
- **BANC - Banca**: comissão que funciona como uma autoridade responsável por determinar o mérito de queixas;
- **CORD - Coordenador**: aquele que define os termos do edital de convocação e coordena a preparação, definindo os membros da banca elaboradora e sorteando as questões da banca que serão efetivamente usadas na avaliação;
- **PDDE - Protocoladora**: Digital de Documentos Eletrônicos:] protocola as mensagens que recebe dos participantes, adicionando a cada mensagem um carimbo de data e hora que fornece referência temporal para as transações;
- **ELAB - Banca elaboradora**: comissão responsável por elaborar as questões, composta por preparadores;
- **FISC - Fiscal**: aquele que está encarregado de iniciar e finalizar a avaliação e fiscalizar os atos dos avaliados durante a avaliação;
- **INSC - Inscrito**: todo e qualquer pré-inscrito que entrega no prazo a documentação necessária para realização da avaliação;
- **QQEU - Qualquer um**: qualquer pessoa que demonstre interesse pelo processo;
- **PART - Participante**: aquele que está inscrito e comparece na avaliação;

- **PREP - Preparador**: aquele que cria as questões e envia para CORD, além de fazer parte (ELAB);

- **PREI - Pré-inscrito**: aquele que se propõe a participar da avaliação manifestando seu interesse em participar ao se registrar para avaliação;

- **INST - Instituição**: entidade responsável por coordenar e supervisionar o processo de avaliação, onde o CORD assina em nome da instituição sempre que isto for necessário;

Como a simples listagem dos participantes de pouco serve para um completo entendimento das necessidades, restrições e características de cada um destes, os usuários tem seus comportamentos apresentados em cada uma das atividades.

6.5 Simbologia Usada no Protocolo

Para poder descrever o protocolo em pseudocódigo, foi necessário definir como as funções criptográficas seriam representadas. A representação escolhida baseia-se em [STA 99] e sua descrição feita para o produto PGP, software para segurança na troca de emails. Os detalhes encontram-se na tabela 6.1.

6.6 Visão Geral do Protocolo

O protocolo para *avaliação segura a distância*, aqui proposto, deve ser visto como um conjunto de protocolos, um para cada atividade do processo, onde cada protocolo define uma ou mais mensagens que devem ser trocadas entre os pares. Cada mensagem possui um formato definido. Pode-se quebrar este protocolo em 3 camadas. A camada mais baixa é responsável pelo serviço de transporte, onde se adota o protocolo *TLS (Transport Layer Security)* para troca de mensagens. Detalhes adicionais sobre esta camada encontra-se na seção6.7. O protocolo *TLS* fornece durante as comunicações certeza de que as mensagens trocadas não estão sendo interceptadas e lidas por terceiros.

Tabela 6.1: Principais funções usadas nos algoritmos que descrevem o protocolo proposto:

Representação	**Observação**
$EP(KU_i, KU_j, msg)$	Cifragem assimétrica usando as chaves públicas e privadas de i e a chave publica de j para cifrar o texto aberto msg
$DP(KU_j, KU_i, c)$	Criptografia assimétrica usando as chaves publicas e privadas de j e a chave publica de i para decifrar o texto c
$EC(K_S, msg)$	Criptografia simétrica usando a chave K_S para cifrar o texto msg
$DC(K_S, c)$	Criptografia simétrica usando a chave K_S para decifrar c
$H(msg)$	Gera o resumo (*hash)*) de msg
$S(KR_i, KU_i, msg)$	i assina a msg
$V(msg, s, KU_i)$	Verifica se a assinatura s é de msg e foi feita por i
$\|\|$	Concatenação

Na camada do meio estão localizados os serviços que lidam com acesso à camada de transporte, recebendo e enviando mensagens. Esta camada interpreta as requisições feitas por clientes remotos e repassa-as para a próxima camada, que realiza o serviço e retorna uma resposta para o intermediário. Esta camada intermediária foi denominada *proxy*. De posse da resposta, o intermediário comunica-se novamente com a camada de transporte e solicita que a resposta seja retornada para o cliente. A terceira, e última camada é responsável por fornecer os serviços de negócio, a saber, convocação e divulgaąão, inscrição, preparação, aplicação, apuração, classificação, publicação e revisão). De modo

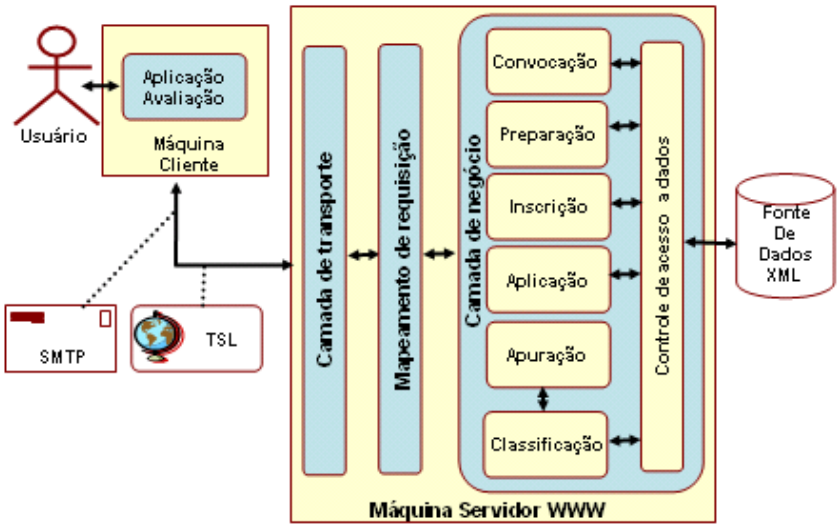

Figura 6.2: Visão geral do protocolo proposto. O protocolo está dividido em 3 camadas sendo a primeira, *camada de transporte*, responsável por realizar as comunicações usando *TLS* ou *SMTP*. Toda requisição feita por um usuário é recebida pela camada de transporte e avaliada na segunda camada e então mapeada para a camada de negócio que irá executar a requisição e acessar a fonte de dados, caso necessário. Feito o processamento a resposta é retornada para a camada de transporte que irá retornar a solicitação para o usuário.

geral, o protocolo está representado na Figura 6.2 e os princípios garantidos por cada uma das camadas são apresentados na Tabela 6.2.

Eronen nota que sistemas distribuídos requerem o uso de técnicas criptográficas enquanto sistemas centralizados podem sobreviver sem esta tecnologia, em [**?**]. Por esta razão, as mensagens são transmitidas por um canal seguro, neste caso *TLS*, e o conteúdo destas deve ser autenticado, ou seja, assinado digitalmente. As mensagens trocadas devem ser armazenadas, servindo de comprovante em caso de disputas. Assume-se que todos participantes, listados na seção 6.4, possuem um par de chaves e um certificado $X.509$, emitido por uma CA confiável. Detalhes podem ser vistos a seguir na subseção 6.6.2.

Tabela 6.2: Princípios garantidos pelas camadas do protocolo. A camada de transporte provê segurança para o canal e a camada de negócio para os documentos armazenados. A camada intermediária do protocolo, *proxy*, possui por objetivo permitir que, caso necessário, a camada de transporte seja alterada sem que haja necessidade de redefinir a camada de negócio, evitando assim a inserção de erros, por tanto, ela não é apresentada na tabela abaixo pois esta camada não influencia os objetivos do protocolo. O princípio da publicidade e da verificabilidade podem ser alcançados através da adoção de um processo que permita a comunidade realizar auditorias e depende da instituição e da comunidade.

Princípio	**Transporte**	**Negócio**
Confidencialidade	X	X
Integridade	X	X
Correta autenticação	X	
Não recusa		X
Igualdade e impessoalidade		X

6.6.1 Controle de Permissões

O controle de permissões, como apresentado por [tACSAC 95, YOU 96], pode ser realizado com o uso de *grupos* ou *papéis*. O termo *grupo* tem sido usado por décadas em sistemas operacionais e aplicativos para se referir a um conjunto de usuários. O controle de acesso baseado em papéis, do inglês *Role-based access control* ou simplesmente *RBAC*, é um modelo adotado para controle de acesso onde papéis unem privilégios e permissões em uma única entidade. As regras de segurança são atribuídas aos papéis e quando os usuários incorporam os papéis adquirem as permissões correspondentes. Por faltar aos grupos uma ligação direta com as permissões, optou-se neste trabalho por especificar os usuários através do modelo *RBAC*, que pode facilmente ser ligado aos atores da *UML* que representam dentro desta papéis. A permissão de cada um dos atores é detalhada dentro de cada uma das atividades do protocolo, encontradas na seção 6.8.

6.6.2 Autenticação e Controle de Acesso

Tradicionalmente, o controle de acesso em sistemas computacionais tem se baseado na verificação da identidade e na verificação do acesso em listas de controle de acesso (*access control list* - *ACL*). Provavelmente, o método mais popular para determinar a identidade seja do uso combinado de nome do usuário e senha. Atualmente aceita-se amplamente a aplicação de certificados digitais, como certificados $X.509$. Um certificado, como visto na subseção 5.2.8, liga uma pessoa ou entidade a uma chave pública. Os certificados podem ser emitidos, por exemplo, pela *UFSC*. O protocolo assume que são confiáveis as seguintes autoridades: Tawte, VeriSign, CertiSign, Certificadora da UFSC. O certificado digital da instituição deve ficar disponível no site em uma página segura, acessível através do protocolo *TLS*, para que possa ser baixado por quem tiver interesse. O protocolo para *avaliação segura a distância*, aqui proposto, não fornece como opção a autenticação de usuários através do uso de nome do usuário e senha, pois esta técnica de autenticação fere o *princípio da não recusa*, especificado anteriormente na subseção 6.2.

O controle de acesso, quando aplicável, é feito através do uso de *ACLs*, onde cada usuário está ligado a um papel. A Figura 6.1 apresenta quem pode participar de uma determinada atividade. No entanto, percebe-se que esta relação é muito genérica, por não fornecer mecanismos para determinação de quais tarefas contam com um papel específico. Além disso, não se especificam quais os privilégios de acesso a documentos são concedidos para o papel dentro da tarefa. Para que aflorem estas informações necessárias para a correta definição do protocolo, as atividades são detalhadas a seguir na seção 6.8, onde pode-se verificar para cada atividade suas tarefas com seus respectivos usuários associados a direitos de acesso.

6.6.3 Documentos

Para poderem ser objeto de transações eletrônicas, os documentos devem estar estruturados de uma forma padronizada. Os documentos são apresentados nas etapas do protocolo em que são pela primeira vez utilizados os formatos.

A padronização pode ser conseguida representando os documentos de acordo com a especificação do padrão *linguagem de marcação extensível* (*xml*) [2], ou no original *extensible markup language*. O padrão XML foi proposto pela W3C (*World Wide Web Consortium - http://www.w3c.org*). O W3C é um consórcio, formado por empresas e instituições, que busca promover e definir padrões para evolução da Web.

Um documento no formato *XML*, como especificado em [MAL 00], é composto por marcações, ou em inglês *tags*. Cada marcação é delimitada por "<"e ">". Toda marcação para ser considerada válida deve ser finalizada (fechada) com o uso de "<"e "/ >". Dentro do padrão *XML* uma marcação correta, ou seja, que foi aberta e fechada é denominada entidade. As entidades não podem conter em seu nome caracteres especiais, definidos no padrão [MAL 00], e não podem ser recursivas. Entidades podem conter atributos para os quais valores são atribuídos. Desta forma, um documento *XML* permite que o seu usuário crie suas próprias marcações e associe valores a estas. O atributo *Uniform Resource Identifiers* ou apenas *URI* identifica um objeto, por exemplo, um arquivo, uma marcação dentro do arquivo *XML*, um endereço de um servidor etc. Um URI, de acordo com [BL 98], define uma sintaxe única e genérica que permite tratar de forma semelhante a localização de diferentes tipos de recursos, mesmo quando o mecanismo de acesso usado para estes recursos divergem entre si. O atributo URI deve seguir a especificação do RFC23962, que pode ser encontrado em [BL 98]. Para visualizar os conceitos descritos recomenda-se ver a figura 6.3. Para cada arquivo XML pode-se associar um arquivo *DTD* que especifica a estrutura do documento XML e quais marcações são obrigatórias.

Um documento no formato XML pode ser transformado em um outro formato qualquer através do uso de uma transformação. Como padrão para realização de transformações recomenda-se o uso de XSLT *Extensible Style Language Transformation*. O processador XSLT lê um documento XML e segue instruções contidas em um arquivo XSL, denominado folha de estilos, e produz então um novo documento em outro formato.

[2] O padrão XML foi escolhido por ser: amplamente usado em transações de comércio eletrônico, fácil de manipular (gerar e ler), fácil de converter para outros formatos.

6.7 Camada de Transporte

Adota-se como solução para a camada de transporte o uso do protocolo *TLS*. O protocolo TLS foi desenvolvido para uso em aplicações cliente/servidor, sendo baseado no protocolo SSL (Secure Socket Layer) versão 3.0. As diferenças entre os dois protocolos não são grandes, entretanto, não há interoperação entre os dois protocolos. O protocolo TLS possui um mecanismo que permite seu rebaixamento para SSL 3.0, o que fornece interoperabilidade entre os dois protocolos. TLS vem sendo amplamente adotado em navegadores, como por exemplo no Microsoft Internet Explorer e no Netscape Navigator. As requisições feitas pelo cliente são enviadas cifradas. O servidor recebe a requisição cifrada e para poder atender a solicitação o servidor decifra a mensagem, requisição, e pode então atender ao cliente. O protocolo TLS suporta o uso de certificados digitais X.509. Então, se necessário, há como autenticar o emissor de uma mensagem, tendo desta forma certeza da origem e da autenticidade das mensagens transmitidas. Este protocolo é aberto, ou seja, pode ser usado, modificado ou melhorado. O protocolo padrão fornece mecanismos para aplicações cliente/servidor realizarem comunicações, de tal forma que uma mensagem só pode ser lida pelos participantes da comunicação. Assim, uma mensagem não pode ser falsificada ou adulterada sem que os participantes percebam. Resumidamente o protocolo provê o seguinte:

- **Canal privado de comunicação** - O protocolo usa criptografia simétrica para cifrar os dados de uma comunicação. A chave usada é válida para cada sessão e é negociada pelo protocolo *TLS Handshake Protocol* que usa criptografia assimétrica;

- **Conexão confiável** - O transporte da mensagem inclui o uso de checagem de integridade, através do uso de funções de resumo;

- **Identificação confiável** - A identidade dos pares pode ser determinada, através do uso de certificados digitais;

- **Extensível** - Fornece um padrão que permite a adoção de novas técnicas criptográficas.

6.8 Camada de Negócio

6.8.1 Convocação e Divulgação

Conforme apresentado na Figura 6.1, a atividade de convocação e divulgação dá início ao processo de avaliação. Nesta atividade o *Coordenador* (*CORD*) está encarregado de definir as regras do edital e selecionar cada um dos membros, ou *preparadores PREP* da *Banca Elaboradora* (*ELAB*) e os Fiscais (*FISC*). As regras devem ser publicadas através de um edital de convocação. A etapa de convocação deve ser realizada para todos os tipos de avaliação apresentados variando apenas quanto ao conteúdo e grau de formalidade requeridos pela legislação. A intersecção entre os modelos de convocação, apresentados no Capítulo 2 demonstra que se deve oferecer sempre, em um edital, no mínimo informações a respeito do seguinte:

- O Programa, indicando as disciplinas e seus conteúdos e bibliografia básica;
- Regras para realização da avaliação:
  - Local
  - Cronograma, quando constituído de diversas etapas;
  - Hora de comparecimento para ingresso no recinto;
  - Hora para início da avaliação;
  - Forma de ingresso, indicando documentação requerida;
  - Condições de realização:
    - Quantoà consulta bibliográfica;
    - Quanto ao uso de máquinas e instrumentos em geral;
- Da classificação e dos recursos;
  - Afixação de gabaritos para fins de recursos, se for o caso;
  - Forma de apresentação de recursos;
  - Vista de prova pelos avaliados;

  - Procedimentos que devem ser seguidos para solicitar revisão;
  - Instância para julgamento de recursos;

- Regras adotadas para correção das avaliações, dando indicação dos métodos de correção para questões de múltipla escolha e subjetivas;

```
<?xml version="1.0" encoding="iso-8859-1" ?>
<envelope>
  <security>
    <signature id="UFSC-SIGNATURE" signedAt="10/01/2002 8h"
      SignatureValueForThisDocument="uri" SignatureMethodAlgorithm="dsa-sha1"
      PublicKeyValue="" />
    <digests DigestMethodAlgorithm="dsa-sha1">
      <digest for="identification" value="j6lwx3rvEPO0vKtMup4NbeVu8nk0" />
      <digest for="rules" value="j6lwx3rvEPO0vKtMup4NbeVu8nk2" />
      <digest for="questions" value="j6lwx3rvEPO0vKtMup4NbeVu8nk1" />
      <digest for="process" value="j6lwx3rvEPO0vKtMup4NbeVu8nk3" />
    </digests>
  </security>
  <assesment>
    <identification>
      <issuer value="UFSC" />
      <description value="" publicAt="02/02/2002" />
    </identification>
    <rules>...</rules>
  </assesment>
</envelope>
```

Figura 6.3: Formato eletrônico para envelope. As regras e os dados da instituição devem ser mantidos dentro de um envelope. O envelope deve ser arquivado cifrado até o momento da sua publicação. Assume-se que CORD é confiável e que por esta razão não divulgará o conteúdo do envelope. O trecho referente às regras foi abreviado. Detalhes do conteúdo das regras encontram-se na Figura 6.4

No entanto *concursos públicos* e *vestibulares* requerem mais informações, conforme visto nas seções 2.2 e 2.3. As informações extras que forem necessárias podem ser adicionadas sem causar nenhum prejuízo ao documento aqui sugerido, na Figura 6.4 tem-se um exemplo da convocação expressa no formato *XML*. O edital de convocação após criado é cifrado e arquivado até o momento da sua publicação. A comunidade pode verificar a autenticidade do documento através da assinatura eletrônica de CORD.

```
<rules>
  <inscription startDate="04/02/2002" startTime="8:00" endDate="05/02/2002" endTime="12:00" />
  <application at="Location - Room 1 - Street xxx - ZIP 99999" startDate="10/02/2002" startTime="8:00" endDate="11/02/2002"
    endTime="12:00" />
  <application-rules>
    <rule>Consulta a material proibida</rule>
    <rule>Uso de calculadora permitido</rule>
  </application-rules>
  <publication date="15/02/2002" at="http://www.?.com.br/enderecogabarito?parametros" />
  <revision requestToAddress="Location - Room 1 - Street xxx - ZIP 99999" requestByEmailToAddress="mail@pro.com.xxx"
    startDate="18/02/2002" startTime="8:00" endDate="20/02/2002" endTime="18:00" />
  <content>
    <topic>
      Historia Geral do Brasil - Ciclos de produção Brasileiros
      <bibliographic-reference>
        <reference type="livro" name="" publication="" author="" editor="" />
        <reference type="artigo" publication="" author="" editor="" />
      </bibliographic-reference>
    </topic>
  </content>
</rules>
```

Figura 6.4: Formato eletrônico para edital de convocação. Este modelo de documento *xml* é completamente extensível, pois, dentro da *tag* regras de aplicacção (*application-rules*) podem ser adicionadas quantas regras (*rule*) forem desejadas pelo preparador. As demais *tags* são de preenchimento obrigatório.

A assinatura e o edital são especificados e arquivados dentro de um envelope. A assinatura pode ser encontrada através da referência feita pela *tag* com nome *signatureValueForThisDocument*. Esta *tag* contém o endereço eletrônico do arquivo que contém a assinatura digital.

A criação do edital digital é feita com os passos a seguir:

1. CORD cria edital de convocação ($EDITAL$);

2. CORD cria formulário de pré-inscrição ($FORMULARIO$);

3. CORD gera e assina o resumo para edital:

   $hEDITAL = H(EDITAL)$

   $sEDITAL = S(KR_{CORD}, KU_{CORD}, hEDITAL)$

4. CORD gera e assina resumo para o formulário de pré-inscrição ($FORMULARIO$):

   $hFORMULARIO = H(FORMULARIO)$

   $sFORMULARIO = S(KR_{CORD}, KU_{CORD}, hFORMULARIO)$

5. CORD arquiva o edital:

   (a) CORD gera de forma randômica uma chave de sessão, K_S;

   (b) CORD cifra a chave de sessão e os documentos:

   $cKS = EP(KU_{CORD}, KU_{CORD}, K_S)$;

   $cEDITAL = EC(K_S, EDITAL)$

   $cFORMULARIO = EC(K_S, FORMULARIO)$

   (c) CORD cria envelope $eEDITAL$:

   $eEDITAL = \{cKS \| cEDITAL \| sEDITAL \|$

   $cFORMULARIO \| sFORMULARIO\}$

   (d) CORD arquiva o envelope ($eEDITAL$);

Na data definida CORD publica o edital seguindo os passos a seguir:

1. CORD decifra a chave des sessão e o conteúdo do edital e do formulário:

   $K_S = DP(KU_{CORD}, KU_{CORD}, SESK)$

   $EDITAL = DC(K_S, cEDITAL)$

   $FORMULARIO = DC(K_S, cFORMULARIO)$

2. CORD publica[3] o edital, o formulário e as assinaturas do edital e do formulário;

6.8.2 Inscrição

No modelo aqui proposto, a assinatura do contrato, tarefa executada por parte de qualquer um (QQEU) que queira se tornar um inscrito (INSC), é obrigatória. Pode-se advogar contra a inclusão desta obrigatoriedade, tendo em vista o fato dela não pertencer ao conjunto das tarefas que compõe o processo da avaliação em sala de aula,

[3]Recomenda-se que o edital seja publicado em um endereço eletrônico acessível através do protocolo HTTPS.

como visto em 2.5. No entanto, a assinatura serve como um comprovante de que o avaliado tomou ciência das regras que irão reger o processo. O comprovante pode ser usado para resolver disputas mesmo em uma *sala de aula*, evitando assim a possibilidade de uma das partes alegar desconhecimento das regras definidas. Adota-se o modelo usado por diversas Instituições, como por exemplo [UDE 01], onde a inscrição é dividida em duas etapas. Na primeira, a pessoa que deseja participar da avaliação manifesta sua vontade seguindo os passos especificados no protocolo e torna-se um pré-inscrito (PREI). Na segunda, o pré-inscrito deve enviar a documentação exigida no edital e passa a ser considerado inscrito (INSC), ou seja, apto a participar da avaliação.

O protocolo inicia quando uma pessoa que deseja participar da avaliação (QQEU) manifesta sua vontade perante a instituição (INST), enviando uma solicitação. A manifestação de vontade deve ocorrer durante um período de inscrição em que o site da instituição está disponível. A pessoa ao se manifestar recebe um envelope contendo as regras definidas no edital de convocação, apresentada na Figura 6.4, e um formulário para ser preenchido com os dados que a instituição precisa para efetivar a inscrição. A regras, que estão assinadas pela instituição, devem ser lidas pela pessoa que, após a leitura, pode ou não aceitá-las, o *aceite* é demonstrado pela geração de uma assinatura para as regras e *não aceite* é representado pela desistência da pessoa. A pessoa para desistir precisa apenas não dar continuidade a nenhuma das demais etapas do protocolo. Feito o aceite a pessoa preenche e assina o formulário de pré-inscrição. O formulário e o comprovante, assinatura gerada para as regras, são colocados em um envelope e retornados para instituição. O envelope recebido pela instituição é aberto e os dados e assinaturas são conferidos. Caso estejam corretos, a pessoa recebe um aviso informando que ela está inscrita na avaliação. O aviso é assinado pela instituição. Caso haja algum erro na assinatura ou nos dados, o candidato recebe um aviso ou mensagem indicando a falha que ocorreu. A pessoa deve refazer a inscrição. Esses aviso também é assinado pela instituição.

O protocolo inicia, portanto, quando uma pessoa solicita a pré-inscrição, seguindo os passos a seguir:

1. QQEU requisita pré-inscrição acessando o endereço eletrônico de INST;

2. INST envia, por um canal seguro, para QQEU as regras e formulário de pré-inscrição:

   $RESPOSTA = \{EDITAL \| FORMULARIO \| sEDITAL \| sFORMULARIO\}$

3. QQEU recebe regras e formulário;

4. QQEU verifica assinatura na mensagem recebida:

   $SIG = (V(EDITAL, sEDITAL, KU_{CORD})$

   $e\ V(FORMULARIO, sFORMULARIO, KU_{CORD}))$

5. Se a assinatura, contida em SIG, não conferir QQEU desiste de seguir o protocolo;

6. Se a assinatura (SIG) for verdadeira continua o processo;

7. QQEU verifica as regras;

8. QQEU decide aceitar as regras:

   (a) QQEU preenche o formulário ($pFORMULARIO$);

   (b) QQEU gera e assina o resumo das regras:

   $hEDITAL = H(EDITAL)$

   $sEDITAL = S(KR_{QQEU}, KU_{QQEU}, hEDITAL)$

   (c) QQEU gera e assina o resumo do formulário preenchido:

   $hFORMULARIO = H(pFORMULARIO)$

   $sFORMULARIO = S(KR_{QQEU}, KU_{QQEU}, hFORMULARIO)$

   (d) QQEU envia formulário e comprovantes:

   $SOLICITACAO = \{pFORMULARIO \| sFORMULARIO \| sEDITAL\}$

Se QQEU decidir não aceitar as regras, ele não dá continuidade no protocolo. Caso seja dada continuidade ao protocolo, a instituição irá verificar se os dados estão corretos. Em caso positivo, QQEU se torna pré-inscrito (PREI), com a instituição indicando desta forma que a solicitação de pré-inscrição foi aceita. O protocolo, da parte da instituição, tem os seguintes passos:

1. INST recebe $SOLICITACAO$;
2. INST verifica $sFORMULARIO$ e $sEDITAL$:

   $SIG = (V(EDITAL, sEDITAL, KU_{QQEU})$

   $e\ V(FORMULARIO, sFORMULARIO, KU_{QQEU}))$
3. Se SIG for verdadeiro e os documentos estão corretos:
   (a) INST prepara mensagem (MSG_ACEITO);
   (b) INST assina a mensagem:

   $sMSG\_ACEITO = S(KR_{INST}, KU_{INST}, MSG\_ACEITO)$

   (c) INST avisa que os dados enviados estão corretos;

   $PRE\_INSCRITO = \{MSG\_ACEITO \| sMSG\_ACEITO\}$

   (d) QQEU recebe $PRE\_INSCRITO$;
   (e) QQEU se tornou PREI;
4. Se SIG for verdadeiro e existe erro nos documentos então:
   (a) INST prepara mensagem (MSG_FALHA) indicando o problema;
   (b) INST assina a mensagem:

   $sMSG\_FALHA = S(KR_{INST}, KU_{INST}, MSG\_FALHA)$

   (c) INST prepara envelope para enviar:

   $eMSG\_FALHA = \{MSG\_FALHA \| sMSG\_FALHA\}$

   (d) INST envia $eMSG\_FALHA$;
   (e) QQEU recebe $eMSG\_FALHA$;
   (f) QQEU volta ao início da pré-inscrição para consertar os erros;
5. Se SIG for falso gerar log da ocorrência;

A inscrição é efetivada quando um pré-inscrito (PREI) envia os documentos exigidos pela instituição (INST), caso os documentos estejam corretos:

1. INST acrescenta os dados de PREI a lista de inscritos ($LISTA\_INSCRITOS$);
2. INST gera e assina resumo para lista:

   $hLISTA\_INSCRITOS = H(LISTA\_INSCRITOS)$

   $sLISTA\_INSCRITOS = S(KR_{INST}, KU_{INST}, hLISTA\_INSCRITOS)$
3. INST gera mensagem de inscrição ($INSCRICAO$), que informa que o PREI está inscrito (INSC);
4. INST gera e assina resumo da inscrição:

   $hINSCRICAO = H(INSCRICAO)$

   $sINSCRICAO = S(KR_{INST}, KU_{INST}, hINSCRICAO)$
5. INST envia $\{INSCRICAO \| sINSCRICAO\}$ para PREI;

Quando os documentos enviados pelo PREI não correspondem ao obrigatório, o PREI é avisado por INST do prazo existente para regularizar a inscrição. A mensagem enviada descreve o problema e deve ser assinada pela INST:

1. INST gera mensagem de inconformidade ($INCONFORMIDADE$), que informa que o PREI não está inscrito ainda;
2. INST gera e assina resumo da mensagem:

   $hINCONFORMIDADE = H(INCONFORMIDADE)$

   $sINCONFORMIDADE = S(KR_{INST}, KU_{INST}, hINCONFORMIDADE)$
3. INST envia $hINCONFORMIDADE$ para uma autoridade de datação (PDDE);
4. PDDE protocola $hINCONFORMIDADE$ e retorna $dINCONFORMIDADE$:
5. INST arquiva $dINCONFORMIDADE$ para casos de litígio;
6. INST envia $\{INCONFORMIDADE \| sINCONFORMIDADE\}$ para PREI;

No final do período de inscrição, a instituição arquiva uma prova da existência da lista de inscritos ($LISTA\_INSCRITOS$), fazendo o seguinte:

1. INST gera e assina resumo para lista de inscritos:

   $hLISTA\_INSCRITOS = H(LISTA\_INSCRITOS)$

   $sLISTA\_INSCRITOS = S(KR_{INST}, KU_{INST}, hLISTA\_INSCRITOS)$

2. INST envia $sLISTA\_INSCRITOS$ uma autoridade de datação (PDDE);

3. PDDE protocola $sLISTA\_INSCRITOS$ e retorna recibo $dLISTA\_INSCRITOS$:

4. INST arquiva $dLISTA\_INSCRITOS$ para casos de litígio;

6.8.3 Preparação

A preparação é uma atividade que, quando encontrada na literatura verificada, visava apenas aos aspectos didáticos de como elaborar questões e provas, sem dar a mínima atenção às características de segurança. Esta atividade consiste basicamente em preparar o material que será usado na execução da avaliação. Ou seja, nesta etapa o material de a avaliação e o gabarito são criados pelo avaliador ou comissão. O gabarito criado deve ser mantido em sigilo até o início da apuração permanecendo durante este período sob a responsabilidade do *Coordenador de preparação* dos resultados e encaminhados para tirar cópias, sendo então os originais e as cópias guardados até o momento que serão novamente necessários.

Um exame, mesmo que superficial, deste processo revela a possibilidade de, durante a cópia, ocorrer um ”vazamento” de informação, pois o responsável por copiar o original possui oportunidade e meios para ler o conteúdo da avaliação, faltando apenas motivo e intenção para isto. No protocolo aqui proposto, a tarefa de cópia é eliminada, por não ser mais necessária, tendo em vista que o processo é executado em meio eletrônico. O processo fica assim:

1. CORD cria a mensagem solicitando a criação de questões:

   $hCRIAR\_QUESTOES = H(CRIAR\_QUESTOES)$

   $sCRIAR\_QUESTOES = S(KR_{CORD}, KU_{CORD}, hC\_QUESTOES)$

   $eCRIAR\_QUESTOES = \{CRIAR\_QUESTOES \| sCRIAR\_QUESTOES\}$

2. CORD comunica cada membro da banca elaboradora (ELAB), enviando o envelope $eCRIAR\_QUESTOES$ que contém a solicitação ($CRIAR\_QUESTOES$);

3. Cada um dos PREP recebe $eCRIAR\_QUESTOES$;

4. Cada PREP retorna mensagem $sCRIAR\_QUESTOES$:

   $hCRIAR\_QUESTOES = H(CRIAR\_QUESTOES)$

   $sCRIAR\_QUESTOES = S(KR_{PREP}, KU_{PREP}, hCRIAR\_QUESTOES)$

5. CORD recebe $sCRIAR\_QUESTOES$ e arquiva para caso de litígio;

Caso qualquer um dos PREP não retorne $sCRIAR\_QUESTOES$ em um período determinado, por exemplo 48 horas, sugere-se entrar em contato direto e verificar o problema. Após verificado o problema, deve-se reenviar $CRIAR\_QUESTOES$.

No prazo definido, cada um dos PREP envia as questões que elaborou conforme o seguinte procedimento:

1. PREP cria a mensagem ($QUESTOES$) contendo as questões;

2. PREP cria a mensagem ($GABARITO$) contendo o gabarito;

3. PREP cria resumo das mensagens e as assinaturas:

   $hQUESTOES = H(QUESTOES)$

   $hGABARTIO = H(GABARITO)$

   $sQUESTOES = S(KR_{PREP}, KU_{PREP}, hQUESTOES)$

   $sGABARITO = S(KR_{PREP}, KU_{PREP}, hGABARITO)$

4. PREP envia proposta ($ePROPOSTA$):

   (a) PREP gera e cifra chave de sessão (K_S);

   $SESK = EP(KU_{PREP}, KU_{CORD}, K_S)$;

(b) PREP gera e cifra proposta de avaliação e o gabarito e coloca-os em $ePROPOSTA$:

$ePROPOSTA\_AVALIACAO = \{QUESTOES \| sQUESTOES\}$

$cPROPOSTA\_AVALIACAO = EC(K_S, ePROPOSTA\_AVALIACAO)$

$eGABARITO = \{GABARITO \| sGABARITO\}$

$cGABARITO = EC(K_S, eGABARITO)$

$ePROPOSTA = \{SESK \| cPROPOSTA\_AVALIACAO \| cGABARITO\}$

5. $ePROPOSTA$ é datada digitalmente;

6. CORD recebe $ePROPOSTA$ e aguarda receber todas questões, ou um conjunto delas;

A criação da avaliação pode ser feita quando as questões forem recebidas. Conforme:

1. CORD para cada mensagem recebida ($ePROPOSTA$):

   (a) CORD decifra a chave de sessão (K_S) e os envelopes;

   $SESK = EP(KU_{CORD}, KU_{PREP}, K_S)$;

   $ePROPOSTA\_AVALIACAO = DC(K_S, cPROPOSTA\_AVALIACAO)$

   $eGABARITO = EC(K_S, cGABARITO)$

   (b) CORD verifica a assinatura em $sQUESTOES$ e $sGABARITO$:

   $SIG = (V(QUESTOES, sQUESTOES, KU_{PART})$

   $e\ V(GABARITO, sGABARITO, KU_{PART}))$

   (c) Se SIG for falso [4]:

   i. descarta $QUESTOES$;

   ii. descarta $GABARITO$;

[4] A verificação pode ser descartada a critério do usuário pois a única maneira de corromper o conteúdo da mensagem ou da assinatura seria obtendo acesso a K_S, o que significa que o sistema como um todo foi comprometido pois a chave privada de um preparador caiu nas mãos de um oponente e ele não comunicou $CORD$ e a autoridade certificadora.

iii. comunica PREP;

(d) Se SIG for verdadeiro:

i. acumula o conteúdo de $QUESTOES$ em $tQUESTOES$;

ii. acumula o conteúdo de $GABARITO$ em $tGABARITO$;

2. Se SIG for falso a mensagem é ignorada;

3. CORD gera e cifra a chave de sessão :

$SESK = EP(KU_{CORD}, KU_{CORD}, K_S)$

4. CORD sorteia as questões da avaliação de $tQUESTOES$ gera $AVALIACAO$;

5. CORD seleciona de $tGABARITO$ as respostas e coloca em $RESPOSTA$;

6. CORD guarda a avaliação em um envelope que contém $AVALIACAO$ e $RESPOSTA$ assinadas e cifradas:

$hAVALIACAO = H(AVALIACAO)$

$sAVALIACAO = S(KR_{CORD}, KU_{CORD}, hAVALIACAO)$

$hRESPOSTA = H(RESPOSTA)$

$sRESPOSTA = S(KR_{CORD}, KU_{CORD}, hRESPOSTA)$

$cAVALIACAO = EC(K_S, \{AVALIACAO \| sAVALIACAO\})$

$cRESPOSTA = EC(K_S, \{RESPOSTA \| sRESPOSTA\})$

$eAVALIACAO = \{SESK \| cAVALIACAO \| cRESPOSTA\}$

7. $eAVALIACAO$ é data digitalmente;

8. CORD arquiva $eAVALIACAO$;

6.8.4 Aplicação

O modelo adotado para aplicação baseia-se na pesquisa apresentada anteriormente na Seção 2.2.8. Em geral, tem-se no local da avaliação a presença de uma pessoa, o avaliador ou um fiscal, que será responsável por garantir o seguinte:

- Acesso apenas às pessoas autorizadas, ou seja, aos avaliados;
- A identidade do avaliado;
- Que o avaliado está portando apenas os itens permitidos durante o processo;
- Nenhum candidato comece a avaliação antes dos demais;
- A permanência dos avaliados no local da prova por um tempo mínimo, como por exemplo dois terços do tempo total destinado à realização da prova;
- A desclassificação dos candidatos ocorrerá sob uma ou mais das seguintes condições satisfeitas:
  - Utilizar ou tentar utilizar-se de meios ilícitos para a resolução da avaliação
  - Contrariar determinações do Fiscal ou cometer qualquer ato de indisciplina durante a realização das provas ;
  - chegar ao Local de Prova após o horário previsto para início ;
  - fornecer indícios para identificação da documentação distribuída ;

Esta etapa inicia quando o inscrito avisa para o fiscal que está presente e prossegue segundo o seguinte procedimento:

1. INSC cria a mensagem informando que está presente ($PRESENTE$);
2. INSC cria e assina o resumo da mensagem:

   $hPRESENTE = H(PRESENTE)$

   $sPRESENTE = S(KR_{INSC}, KU_{INSC}, hPRESENTE)$
3. INSC avisa FISC que está presente:

   $ePRESENTE = \{PRESENTE \| sPRESENTE\}$

Os fiscais (FISC[5]) aguardam chegada de inscritos até o início da avaliação. Para cada inscrito (INSC) que dá sinal de presença, o fiscal age conforme detalhado a seguir:

1. FISC recebe mensagem contendo $ePRESENTE$;
2. Se a assinatura conferir e o nome constar na lista de inscritos e prazo não expirou e mensagem não for repetida, faz-se o seguinte:
   (a) FISC acrescenta dados de INSC á ata (ATA);
   (b) FISC envia aviso de aceite de entrada ($ENTRADA$) para INSC;
   (c) FISC cria e assina resumo da mensagem e coloca em um envelope:
   $hENTRADA = H(ENTRADA)$
   $sENTRADA = S(KR_{FISC}, KU_{FISC}, hENTRADA)$
   $eENTRADA = \{ENTRADA \| sENTRADA\}$
   (d) FISC envia $eENTRADA$ para INSC;
   (e) INSC recebe a mensagem e verifica autenticidade:
   $SIG = V(ENTRADA, sENTRADA, KU_{FISC})$
   (f) Se SIG for verdadeira então INSC se torna um participante (PAR);
   (g) Se INSC não receber mensagem de que é um participante (PAR), dentro de um tempo aceitável, deve reiniciar o processo;
3. Se a assinatura não conferir ou o prazo expirou ou a mensagem é repetida, descarta a mensagem e gera log.

Cada um dos fiscais (FISC) no horário do início da avaliação entregam as atas (ATA) para o coordenador e aguardam a avaliação que deve ser distribuída para os participantes (PAR), de acordo com o seguinte procedimento:

[5]Este serviço pode ser colocado no ar quando houverem avaliações a serem executadas. Obedecendo para isto a antecedência de tempo definida no edital por exemplo, equivalendo ao processo tradicional de indicar para os inscritos quanto tempo antes podem começar a chegar para a avaliação.

1. FISC cria e assina o resumo da ata:

   $hATA = H(ATA)$

   $sATA = S(KR_{FISC}, KU_{FISC}, hATA)$

2. FISC envia $hATA$ para uma autoridade de datação (PDDE);

3. PDDE recebe, protocola a mensagem $hATA$ e retorna $dATA$;

4. FISC recebe $dATA$;

5. FISC envia para CORD a prova de presença ($eATA$):

   $eATA = \{ATA \| sATA \| dATA\}$

6. CORD recebe $eATA$ e verifica as assinaturas;

7. Se as assinaturas estão corretas, CORD autoriza início da avaliação, quando for a data e hora definidos;

8. Se as assinaturas não estão corretas CORD, gera log da ocorrência.

Quando for o momento de iniciar a avaliação, cabe a CORD distribuir as avaliações para os fiscais, que, por sua vez, irão entregá-las para os participantes que estão aguardando desde o momento que indicaram que estão presentes. O processo é detalhado abaixo:

1. CORD recupera a avaliação do envelope:

   (a) CORD decifra a chave de sessão a partir de ($SESK$) do envelope ($eAVALIACAO$):

   $K_S = DP(KU_{CORD}, KU_{CORD}, SESK)$;

   (b) CORD retira $cAVALIACAO$ de $eAVALIACAO$;

   (c) CORD decifra o conteúdo de $cAVALIACAO$:

   $tAVALIACAO = DC(K_S, cAVALIACAO)$

   (d) CORD recupera de $tAVALIACAO$ o conteúdo de $\{AVALIACAO \| sAVALIACAO\}$

2. CORD, para cada FISC que solicitar, gera uma chave de sessão K_S;

   (a) CORD cifra questões para FISC:

   $cQUESTOES = EC(K_S, AVALIACAO)$

   (b) CORD recupera $sAVALIACAO$;

   (c) CORD envia uma mensagem contendo as questões:

   $eQUESTOES = \{K_S \| sAVALIACAO \| cQUESTOES\}$;

   (d) FISC recebe $eQUESTOES$;

   (e) FISC autoriza os avaliados a começarem a avaliação.

Quando o início da avaliação é autorizado por FISC, seguem-se os passos a seguir:

1. FISC envia para cada um dos PART a mensagem $eQUESTOES$;

2. PART recebe avaliação $eQUESTOES$;

3. PART não recebe avaliação $eQUESTOES$ no tempo previsto e solicita envio;

4. PART protocola recebimento enviando o seguinte:

   (a) PART recupera K_S;

   (b) PART decifra $cQUESTOES$:

   $QUESTOES = DC(K_S, cQUESTOES)$

   (c) PART calcula e assina o resumo de $QUESTOES$:

   $hQUESTOES = H(QUESTOES)$

   $sQUESTOES = S(KR_{PART}, KU_{PART}, hQUESTOES)$

   (d) PART envia resumo assinado;

   (e) FISC recebe e arquiva o resumo assinado $sQUESTOES$;

5. PART responde as questões e gera $RESPOSTA\_QUESTOES$;

Depois de cada participante (PART) ter respondido as questões, ele prossegue o protocolo entregando as respostas para o fiscal, seguindo o processo de entrega a seguir:

1. PART envia avaliação para FIS, contida em $eRESPOSTA\_QUESTOES$:
   (a) PART preenche seção de identificação da avaliação e gera $IDENTIFICACAO$;
   (b) PART gera e assina os resumos:
   $hRESPOSTA\_QUESTOES = H(RESPOSTA\_QUESTOES)$
   $sRESPOSTA\_QUESTOES = S(KR_{PART}, KU_{PART}, hRESPOSTA\_QUESTOES)$
   $hIDENTIFICACAO = H(IDENTIFICACAO)$
   $sIDENTIFICACAO = S(KR_{PART}, KU_{PART}, hIDENTIFICACAO)$
   (c) PART cifra $IDENTIFICACAO$ para CORD:
   $cIDENTIFICACAO = EP(KU_{PART}, KU_{CORD}, IDENTIFICACAO)$;
   (d) PART gera envelope com a identificação:
   $eIDENTIFICACAO = \{cIDENTIFICACAO \| sIDENTIFICACAO\}$
   (e) PART gera versão final da avaliação:
   $eRESPOSTAS = \{RESPOSTA\_QUESTOES \|$
   $sRESPOSTA\_QUESTOES \| eIDENTIFICACAO\}$
2. FISC recebe $eRESPOSTAS$;
3. FISC data digitalmente $eRESPOSTA$;
4. FISC confirma recebimento enviando:
   $COMPROVANTE = S(KR_{PART}, KU_{PART}, H(eRESPOSTAS))$
5. PART arquiva $\{eRESPOSTAS \| COMPROVANTE\}$;

Alternativamente ao cenário acima tem-se a possibilidade de o tempo para entrega estar finalizando, faltando por exemplo 15 minutos para o final, e alguns dos participantes (PART) não entregaram ainda a avaliação. FISC informa o prazo para PART entregar a avalição. Neste caso:

1. FISC envia mensagem para PART informando o final do tempo:
   (a) FISC cria mensagem de tempo esgontado $ESGOTANDO$;
   (b) FISC assina mensagem:
   $sESGOTANDO = S(KR_{PART}, KU_{PART}, H(ESGOTANDO))$
   (c) FISC envia $\{ESGOTANDO \| sESGOTANDO\}$ para PART;
2. PART recebe aviso;
3. PART entrega as respostas dentro do prazo (seguindo o processo de entrega);

Finalizado o tempo máximo estipulado para aceite das avaliações respondidas, mesmo se algum participante ($PART$) não tenha entregue suas respostas, o fiscal finaliza o processo:

1. Para cada $eRESPOSTAS$ recebido no prazo:
   (a) FISC calcula o resumo de $eRESPOSTAS$:
   $hRESPOSTAS = H(eRESPOSTAS)$
   (b) FISC acumula respostas em $eAVALIACOES$:
   $eAVALIACOES = \{eRESPOSTAS \| COMPROVANTE \| hRESPOSTAS\}$;
   (c) AVAL confirma recebimento de $eAVALIACOES$;
2. Se CORD não receber $eAVALIACOES$ no tempo previsto deve comunicar FISC;

Para cada um dos participantes que não entregaram a avaliação, o fiscal (FISC) deve gerar um mensagem indicando que não foi feita a entrega. Esta mensagem deve ser verificada e protocolada por PDDE. A mensagem é enviada para o participante que não fez a entrega e o coordenador recebe uma lista contendo informações sobre todas mensagens enviadas:

1. FISC gera aviso de não recebimento $NAO\_ENTREGUE$. O aviso deve conter informações que permitam a identificação de PART;

2. FISC calcula e assina o resumo de $NAO\_ENTREGUE$:

   $hNAO\_ENTREGUE = H(NAO\_ENTREGUE)$

   $sNAO\_ENTREGUE = S(KR_{FISC}, KU_{FISC}, hNAO\_ENTREGUE)$

3. FISC envia $hNAO\_ENTREGUE$ para PDDE;

4. PDDE retorna protocolo $dNAO\_ENTREGUE$;

5. FISC arquiva protocolo;

6. FISC cria envelope:

   $eNAO\_ENTREGUE = \{NAO\_ENTREGUE \| sNAO\_ENTREGUE\}$

7. FISC envia $\{eNAO\_ENTREGUE \| dNAO\_ENTREGUE\}$ para CORD e PART;

6.8.5 Apuração e Classificação

A convocação determina os critérios adotados durante a apuração. Alguns exemplos desses critérios podem ser observados na subseção 2.2.9. Esta etapa é crítica, pois erros cometidos nela podem causar prejuízos ao avaliado que pode, por exemplo, receber uma pontuação menor do que aquela à qual tem direito. A apuração deve, portanto, ser executada de forma impessoal, ou seja. Sem que o nome do candidato seja de conhecimento das pessoas envolvidas na correção. A classificação por sua vez consiste em aplicar os critérios definidos na convocação e determinar para cada avaliado o seu desempenho. Esta atividade é aplicável apenas quando se trata de uma avaliação que tem por objetivo escolher o melhor ou melhores avaliados e deve ser executada de forma impessoal, como na apuração. Na classificação podem ser aplicados pesos aos resultados parciais obtidos pelos candidatos em outras etapas. A classificação pode depender da média ou de outros fatores como títulos ou presença de deficiência física.

A apuração inicia quando o avaliador (AVAL) recebe o gabarito, seguindo os passos a seguir:

1. AVAL recebe as avaliações ($eAVALIACOES$), onde:

$eAVALIACOES = \{eRESPOSTAS_1, eRESPOSTAS_2,$

$eRESPOSTAS_{...}, eRESPOSTAS_n\}$;

2. CORD envia o gabarito para AVAL:

   (a) CORD recupera a avalição de um envelope que contém $AVALIACAO$ e $RESPOSTA$ assinadas e cifradas:

   $eAVALIACAO = \{SESK \| cAVALIACAO \| cRESPOSTA\}$

   $K_S = DP(KU_{CORD}, KU_{CORD}, SESK)$

   $aAVALIACAO = DC(K_S, \{AVALIACAO \| sAVALIACAO\})$

   $aRESPOSTA = DC(K_S, \{RESPOSTA \| sRESPOSTA\})$

   (b) CORD envia $aRESPOSTA$ para AVAL:

3. Calcula e assina o resumo de RESPOSTA:

   $hRESPOSTA = H(RESPOSTA)$;

   $sRESPOSTA = H(RESPOSTA)$;

4. AVAL envia $sRESPOSTA$ para CORD;

5. CORD arquiva $sRESPOSTA$;

Recebido o gabarito e as avaliações enviadas pelos fiscais o avaliador para cada avaliação atribui nota, conforme o seguinte procedimento:

1. AVAL recupera $RESPOSTA\_QUESTOES$ de $eRESPOSTAS_1$;

2. AVAL corrige as respostas ($RESPOSTA\_QUESTOES$) de acordo com o gabarito ($RESPOSTA$);

3. AVAL determina nota ($NOTA$);

4. AVAL calcula e assina:

   $hRESULTADO = H(RESPOSTA\_QUESTOES)$;

$sRESULTADO = S(KR_{AVAL}, KU_{AVAL}, hRESULTADO)$

$sNOTA = S(KR_{AVAL}, KU_{AVAL}, H(NOTA))$

5. AVAL envia $RESULTADO$ para $CORD$:

   $RESULTADO = \|NOTA\|sRESULTADO\|sNOTA\}$

6.8.6 Publicação

Para concursos públicos e vestibulares recomenda-se o agrupamento e publicação dos resultados em uma página web segura. Os resultados podem ser publicados depois que o seguinte for feito:

1. Para cada resultado recebido, CORD faz o seguinte:
   (a) Verifica assinatura de AVAL;
   (b) Ordena os resultados;
2. Para cada resultado i recebido CORD faz adicionalmente o seguinte:
   (a) Recupera a identidade de PARTi;
   (b) Informa PART de seu resultado[6] com o envio de
   $RESULTADOi$:
   $RESULTADO$

6.8.7 Revisão

Após o candidato verificar o resultado e conferir sua Avaliação no processo de Publicação, ele pode requisitar uma revisão da avaliação quando acreditar que existem erros na correção que foi realizada de acordo com o apresentado na subseção 6.8.5. Na revisão deve constar onde o avaliado considera que houve erro na correção que foi realizada durante a etapa de Apuração . Caso um erro seja identificado, o gabarito

[6]Que pode incluir a colocação no caso de um concurso.

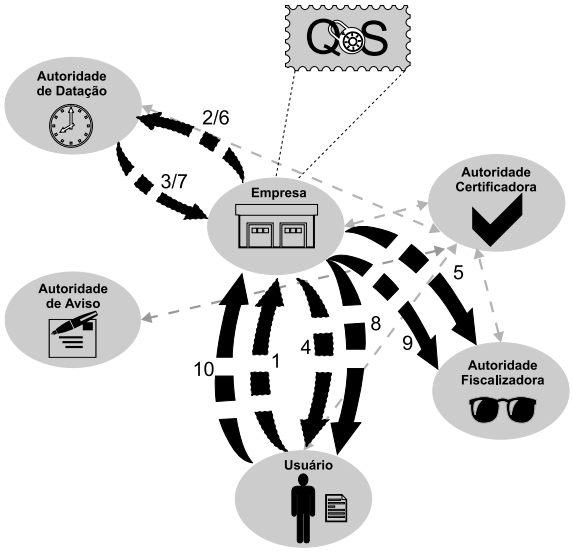

Figura 6.5: Funcionamento do processo de revisão. 1. **CL** faz a requisição; 2. **EM** envia o recibo da requisição para **PDDE**; 3. **PDDE** protocola o recibo e devolve-o para **EM**; 4. **EM** envia o recibo de requisição para **CL**; 5. **EM** envia uma cópia do recibo de requisição para **AF**; 6. Após concluir a **OS** gerada com a requisição do **CL**, **EM** gera um documento para o fechamento da **OS** e envia para **PDDE**; 7. **PDDE** protocola o documento para o fechamento da **OS** e envia para **EM**; 8. **EM** envia uma solicitação de fechamento da **OS** para **CL**; 9. **EM** envia uma cópia da solicitação de fechamento da **OS** para **AF**; 10. **CL** analisa a solicitação e responde fechando o ciclo da transação.

e a avaliação dos demais candidatos devem ser revistos conforme apresentado na Figura 2.8. Neste caso, a apuração, classificação e publicação devem ser refeitas e todos os candidatos informados do que ocorreu.

As requisições para revisão normalmente são aceitas apenas quando feitas dentro de um prazo estipulado, sendo que este prazo deve estar especificado na Convocação, conforme anteriormente definido na subseção 6.8.1. Optou-se aqui por adotar na etapa de revisão o protocolo criado no Laboratório de Segurança em Computação (LabSEC), do Curso de Pós-graduação em Computação da Universidade Federal de Santa Catarina, por Ghisleri [GHI 02]. O protocolo de Ghisleri, denominado *Sistema Seguro de Atendimento ao Cliente*

Garantia da Qualidade de Serviço garante a qualidade do serviço no atendimento aos

clientes, levando em consideração as questões de segurança. Para se entender claramente este protocolo, deve-se atentar para a notação utilizada dentro deste para as mensagens trocadas entre os participantes do protocolo. A identificação dos elementos encontra-se na relação abaixo:

- **CL - Cliente**: usuário do protocolo, um inscrito;
- **EM - Empresa**: quem adota o protocolo, a instituição;
- **PDDE - Autoridade de Datação**: responsável por protocolar os recibos das requisições e os de fechamento;
- **AF - Autoridade Fiscalizadora**: mediadora dos eventuais litígios entre o cliente e a empresa;
- **AC - Autoridade Certificadora**: provedora dos certificados digitais para a identificação dos elementos participantes;
- **AA - Autoridade de Aviso**: responsável pela notificação do cliente através de diversos meios de comunicação;
- **REQ - Requisição**: que é assinada digitalmente pelo cliente e enviada para a empresa;
- **OS - Ordem de Serviço**: gerada pela empresa para atender a requisição enviada pelo cliente;
- **RR - Recibo da Requisição**: mensagem composta pela requisição do cliente e o protocolo gerado pela autoridade de datação; serve como comprovante;
- **FEC - Fechamento**: ordem de serviço assinada digitalmente pela empresa e protocolada pela autoridade de datação. Serve como garantia para a empresa de que efetuou o serviço naquele determinado prazo;
- **RF - Recibo de Fechamento**: gerado pelo cliente com a sua assinatura na mensagem de fechamento da ordem de serviço recebida da empresa.

Observando, então, os passos numerados na Figura 6.5, tem-se o seguinte:

1. O cliente (inscrito) é o ponto de partida do protocolo, quando através de uma visita ao web site da instituição solicita a inscrição, através de uma requisição assinada digitalmente por ele de forma a garantir a sua identidade;

2. A empresa (instituição) recebe a requisição, gera um resumo da mensagem com um algoritmo de *hash*, assina digitalmente e o encaminha para a autoridade de datação;

3. A autoridade de datação recebe o resumo da mensagem enviada pela instituição, protocola acrescentando data e hora locais e devolve para a instituição tudo assinado digitalmente. Com isso, é gerado o protocolo que comprova a requisição feita pelo inscrito;

4. A empresa recebe o protocolo solicitado à PDDE e gera o recibo da requisição para o inscrito, dando-lhe com isso, a garantia para o atendimento. Esse recibo é composto pela requisição do inscrito concatenada com o protocolo emitido pela PDDE. Paralelamente, uma ordem de serviço (OS) é aberta na empresa para atender a requisição do cliente;

5. Uma cópia do recibo também é remetida para a autoridade fiscalizadora, que o armazena em seu banco de dados para eventuais auditorias ou até mesmo litígio entre os participantes. Neste passo, a fase de requisição se encerra.

6. A empresa, após atender e concluir a ordem de serviço referente á requisição do cliente, efetua o fechamento da mesma, gera um resumo (*hash*) e o envia para a autoridade de datação;

7. A PDDE protocola o resumo de fechamento da OS e devolve para a instituição. O fato de se protocolar esse fechamento, dá à instituição a comprovação do atendimento ao cliente naquele determinado prazo;

8. A empresa recebe o protocolo de fechamento da OS e gera o comprovante de fechamento (FEC), despachando-o juntamente com uma mensagem para o cliente.

Essa mensagem solicita ao cliente o encerramento da transação iniciada por ele junto à empresa;

9. Uma cópia do FEC é enviada também para a autoridade fiscalizadora, o que permite a confrontação com o recibo de requisição para se verificar o prazo no atendimento. A autoridade fiscalizadora, poderá fazer isso a qualquer momento, seja a título de auditoria ou reclamação;

10. O inscrito, após verificar o atendimento recebido, encerra a transação com a sua assinatura na mensagem de fechamento recebida da empresa. Com essa operação, tem-se o recibo de fechamento, que é a garantia da empresa junto ao protocolo. Dessa forma, conclui-se idealmente uma transação prevista no protocolo.

Como pôde ser verificado, o protocolo proposto por [GHI 02] elege uma autoridade fiscalizadora que pode acompanhar e intervir no processo de atendimento ao cliente, caso seus direitos sejam ameaçados. Tal autoridade fiscalizadora pode ser o próprio setor de garantia da qualidade da empresa, ou um órgão do governo que deseje monitorar as atividades de uma concessão de serviço público. Verifica-se ainda que o protocolo faz uso de um canal seguro e que as mensagens são sempre que necessário assinadas e protocoladas. Em [GHI 02] pode-se encontrar a formalização do protocolo.

6.9 Conclusão

As técnicas de criptografia usadas permitem que o protocolo garanta o seguinte:

- Os avaliados não tem como acessar as questões antes da data e hora marcados;
- Os avaliados não tem como acessar o gabarito antes da data e hora marcados;
- Um avaliado não tem como responder as questões em uma data e hora diferentes do estabelecido para a realização da avaliação, pois ele precisaria para isto da conivência dos fiscais e do coordenador.

- As respostas não podem ser alteradas após a avaliação ter sido entregue, pois o resumo da avaliação entregue é assinado pelo fiscal e protocolado por uma autoridade datação.

Sendo assim, o protocolo apresentado atende aos princípios legais e computacionais anteriormente apresentados na abertura deste capítulo. A seguir apresenta-se argumentações nesse sentido para cada requisito de segurança apresentado na seção 2.1:

- **Igualdade e impessoalidade** - Na apuração não há como o avaliador determinar qual avaliação esta corrigindo pois a identificação da avaliação é cifrada com a chave publica do coordenador. Durante a publicação, por sua vez, a nota publicada deve ter sido assinada pelo avaliador. As técnica de criptografia empregadas são aceitas pela comunidade científica e empresarial como seguras.

- **Publicidade** - Os resultados, o protocolo e os programas usados no processo são públicos e ficam disponíveis para avaliação e modificação;

- **Verificabilidade** - As avaliações podem ser verificadas manualmente por quem desejar, tendo em vista que o gabarito usado na atividade de publicação é disponiblizado para a comunidade;

- **Confidencialidade** - As mensagens trocadas entre os pares trafegam por um canal de segurança comprovada;

- **Integridade** - As mensagens enviadas em uma comunicação são transmitidas de forma fiel. Esta garantia é fornecida pela camada de transporte;

- **Correta autenticação** - A autenticação das partes é feita usando-se certificados digitais trocados na inicialização das comunicaçõe (camada de transporte). O certificado digital das partes serve como garantia da identidade, e se mais controle for necessário pode-se adotar o protocolo de [FIO 00];

- **Não recusa** - As mensagens são assinadas digitalmente e quando necessário são arquivadas para servirem como prova em casos de litígio.

Ressalta-se ainda que apenas o coordenador tem acesso ao conteúdo de todas questões e do gabarito e que, quanto maior o número de preparadores e de questões criadas, maior tende a ser a segurança oferecida.

Capítulo 7

Formalização do Protocolo

7.1 Introdução

O capítulo anterior apresentou um modelo de protocolo que fornece validade jurídica e segurança dos documentos usados na avaliação do conhecimento, tendo a Internet como meio de transmissão. O protocolo proposto foi descrito conforme as fases de sua utilização, porém, a formalização do modelo se torna assim necessária. Uma representação matemática do protocolo proposto pode ser usada para criar, manter, analisar, simular e validar o funcionamento e eficácia deste. Neste capítulo usam-se redes de Petri para formalizar o protocolo anteriormente apresentado.

7.2 Redes de Petri

Redes de Petri foram propostas em 1962 como uma maneira de modelar sistemas com concorrência. Segundo [JC 97], adaptam-se bem a um grande número de situações onde a evolução de eventos são importantes, tais como representação de tarefas de montagem, concepção de softwares distribuídos, concepção de softwares de tempo real, modelagem e análise de protocolos etc. As redes de Petri, conforme [JC 97], são formadas basicamente pelos três elementos a seguir:

Lugar - Representado por um círculo, tem em geral um predicado associado;

Transição - Representada graficamente por uma barra ou um retângulo, expressa um evento que ocorre no sistema;

Ficha - Representada por um ponto dentro do lugar, pode determinar uma condição do lugar onde se encontra.

Os lugares e fichas descrevem entidades abstratas como condições ou estados, podendo ainda descrever entidades físicas como peças ou depósitos. Existindo uma ficha dentro de um lugar, a condição representada por este lugar é considerada verdadeira. De forma geral, os lugares possuem um predicado, tais como tempo esgotado, não entregue e site disponível.

A ocorrência de um evento em um rede Petri é representada pelo disparo de uma transição. Ou seja, as fichas são retiradas da entrada e depositadas em cada lugar da saída. Quando as fichas saem da entrada, a situação indicada por elas não é mais verdadeira, ou seja, o lugar está vazio.

As Redes de Petri possuem as seguintes propriedades, de acordo com [ESP 94]:

- **Em conflito estrutural** - Duas transições estarão em conflito estrutural se e somente se elas tiverem ao menos um lugar de entrada em comum;
- **Em conflito efetivo** - Duas transições estão em conflito efetivo para uma marcação se e somente se ambas estão em conflito estrutural e estão sensibilizadas;
- **Com Paralelismo estrutural** - Duas transições são paralelas se não possuem nenhum lugar de entrada em comum;
- **Com paralelismo efetivo** - Duas transições são paralelas se não possuem nenhum lugar de entrada em comum;
- **Livre de Deadlock**[1] - Se para cada marcação alcançável alguma transição é habilitada;

- **Home states** - Uma marcação de uma Rede Petri esta em *home state* se ela é alcançável a partir de cada um dos estados alcançáveis;

- **Persistente** - Se para quaisquer duas transições diferentes habilitadas a ocorrência de uma não desabilita a outra.

As redes podem ainda ser agrupadas em classes, conforme [ESP 94], da seguinte forma:

- **Pura** - Para todas as transições, não existe nenhum lugar que esteja, ao mesmo tempo, na entrada e na saída;

- **Viva** - A vivacidade refere-se ao disparo das transições. Uma transição é viva se, a partir de qualquer estado do grafo gerado, existe uma seqüência de disparos que a contenha, ou seja, que leve a seu disparo. Uma transição é quase-viva se foi disparada ao menos uma vez durante a construção do grafo.

- **Limitação** - É calculado o número máximo de fichas (limite) em cada lugar da rede, para os estados alcançáveis. Os lugares podem ser nulos, quando nunca recebem fichas; binários, sempre possuindo uma ou nenhuma ficha; limitados, quando o número de fichas é sempre igual ou inferior a um limite finito maior que 1; ou não limitados, quando o número de fichas tende ao infinito;

- **Reiniciável** - A rede é reiniciável se todos os seus estados forem reiniciáveis. Um estado é reiniciável se, partindo dele, existe alguma seqüência de disparos de transições que leve de volta ao estado inicial.

- **Segura** - Nenhuma marcação possui mais de uma ficha em um lugar;

7.3 Etapas do Processo

Todas as etapas do protocolo foram modeladas e avaliadas pela ferramenta DaNaMics, versão beta 1.1, que foi escolhida com base nos comparativos feitos

[1]Não ocorre paralisação funcional.

pelo site *http://home.arcor-online.de/wolf.garbe/petrisoft.html*, que lista características de 98 ferramentas. DaNaMics foi escolhida por ser capaz de modelar, analisar e verificar as redes de Petri com o adicional de ser gratuita e multiplataforma. As características encontradas nos modelos apresentados mais adiante neste capítulo podem ser vistas na Tabela 7.1

Tabela 7.1: Principais características das redes do protocolo. Conforme os resultados apontados pelo programa utilizado para a análise e modelagem da rede, pode-se destacar as características abaixo para todos os modelos:

Característica Avaliada	**Observação**
Viva	Sim, pois todas transições são disparáveis
Reiniciável	Não, pois analisando o grafo da rede, pode-se observar que as marcações iniciais não recebem nenhuma entrada de outro caminho
Livre de Deadlock	Sim, pois para todas marcações habilitadas alguma transição é habilitada
Possui *home states*	Sim, pois para todas marcações habilitadas alguma transição é habilitada
Segura	Sim, nenhum lugar recebe mais de uma ficha
Limitação	Os lugares são binários
Persistente	Sim, nenhuma transição desabilita outras

7.3.1 Convocação

A convoção, conforme visto anteriormente na subseção 6.8.1, está dividida nas duas partes seguintes:

- Criação do edital, onde o coordenador define as regras e guarda-as cifradas até o momento da publicação. Está representada na Figura 7.1;

- Publicação do edital, onde o coordenador decifra e torna público o conteúdo do edital. Encontra-se detalhada na Figura 7.2;

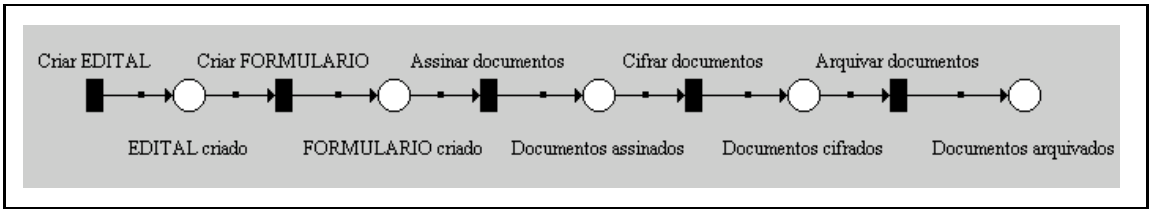

Figura 7.1: Criação do edital

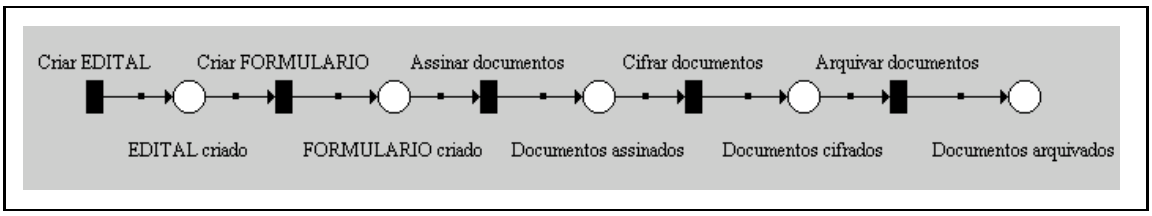

Figura 7.2: Publicação do edital

7.3.2 Inscrição

A inscrição, conforme pode ser percebido pela leitura da subseção 6.8.2, está dividida em três possibilidades:

- Requisição de pré-inscrição, visto na Figura 7.3, onde uma pessoa qualquer solicita o formuário e o edital. Se a pessoa concorda com os termos do edital, ela preenche o formulário e o envia para a instituição;

- Pré-inscrito envia os documentos para serem analisados pelas instituição, que irá analisar a documentação e determinar se a pessoa irá passar de pré-inscrito para inscrito. Existem três casos a seguir:

  – Quando a inscrição pode ser efetivada, apresentada na Figura 7.4;

  – Quando a inscrição pode não ser efetivada, apresentada na Figura 7.5;

- Término do período inscrição, representada pela Figura 7.6;

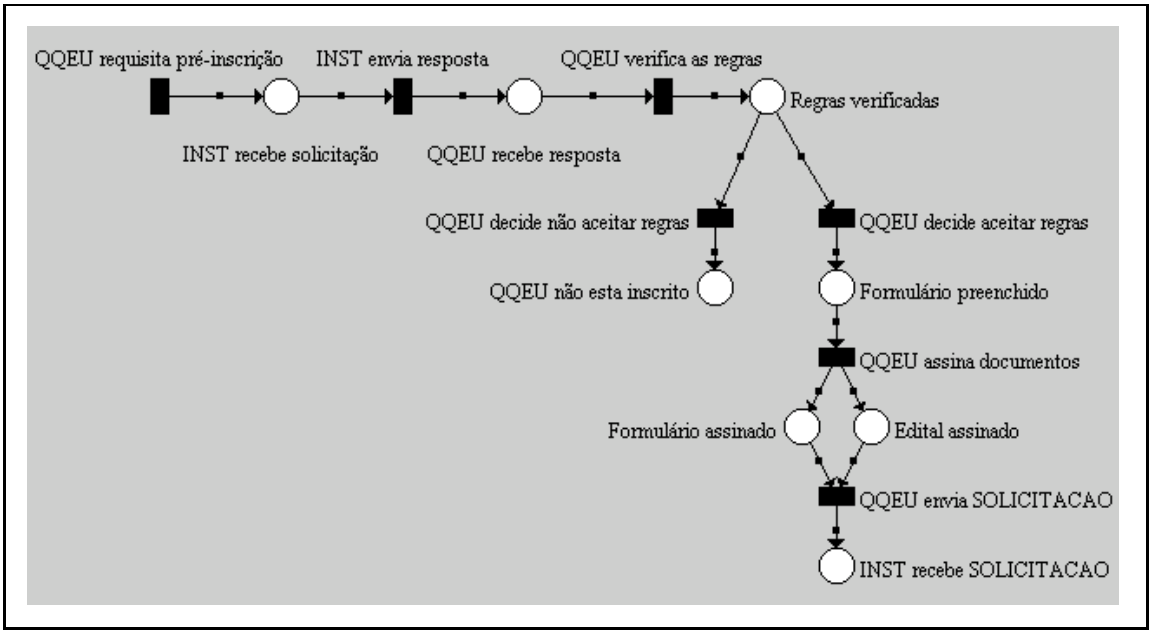

Figura 7.3: Requisição pré-inscrição

7.3.3 Preparação

A etapa de preparação, modelada na subseção 7.3.3, divide-se nas três seguintes partes:

- Coordenador solicita para preparador a criação da avaliação, conforme mostrado na Figura 7.7;
- Preparador envia proposta de questões e gabarito para o coordenador, ilustrada na Figura 7.8;
- Coordenador prepara e arquiva avaliação cifrada, conforme passos descritos anteriormente e, conforme Figura 7.9, quando considerar necessário antes da aplicação a avaliação que será aplicada é preparada.

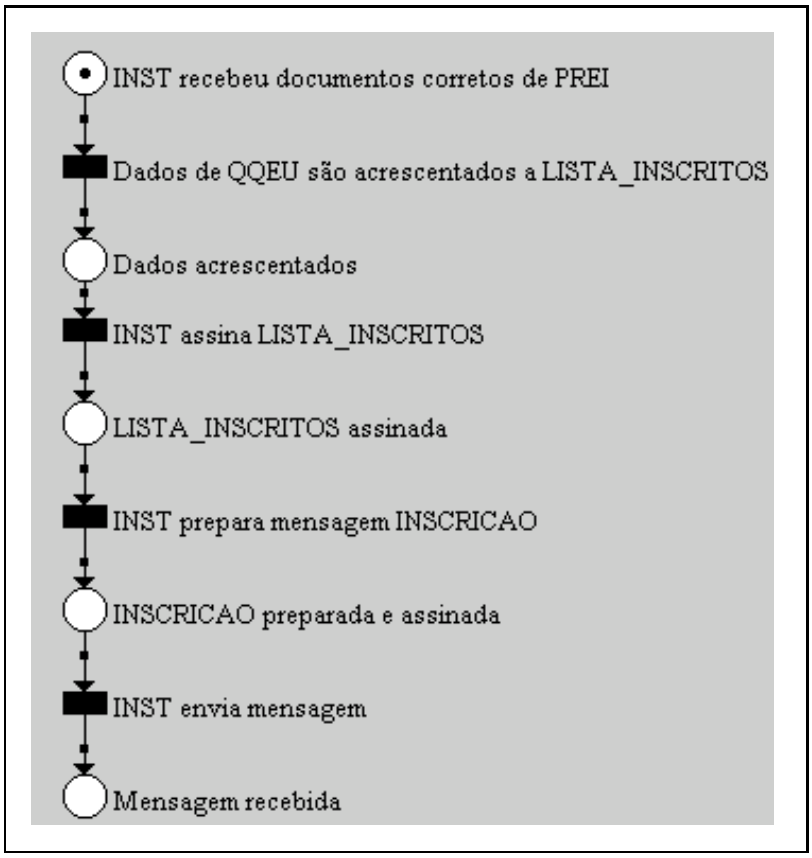

Figura 7.4: Inscrição efetivada

7.3.4 Aplicação

A aplicação divide-se em diversos subprotocolos, conforme pode ser observado na subseção 6.8.4, onde se tem o seguinte:

- Aviso de presença emitido por cada um dos inscritos que ”comparecem” para a avaliação.

- O aviso é recebido por um fiscal que irá autorizar ou não a participação de quem emitiu o aviso, incluindo ou não o nome na ata. De forma resumida o processo pode ser visto na Figura 7.10;

- Quando o prazo de entrada expira, o fiscal arquiva a ata, seguindo os passo da Figura 7.11;

- Quando o prazo de entrega para as resposta se torna próximo, o fiscal avisa os participantes que ainda não entregaram suas respostas do tempo que eles têm disponível, seguindo os passos da Figura 7.14;
- O coordenador autoriza o início da avaliação, entregando as ”provas” para os fiscais, que por sua vez entregam estas para os participantes, conforme mostrado na Figura 7.12;
- O participante envia as respostas segundo os passos apresentados na Figura 7.13;
- Esgotado o prazo, o fiscal deve registrar as avaliações não entregues, conforme ilustrado na Figura 7.15;

7.3.5 Apuração e Classificação

A apuração é realizada por um avaliador que recebe as avaliações enviadas pelo fiscal. Durante a apuração o avaliador não tem como verificar a identidade do avaliado, pois a identificação deste foi cifrada, usando criptografia assimétrica, e somente o coordenador pode verifica-la. Garante-se assim o princípio da igualdade. O processo de apuração é detalhado na Figura 7.16.

7.4 Conclusão

O emprego de Redes de Petri foi útil na definição do funcionamento do protocolo, pois permitiu eliminar os *deadlocks* que existiam em versões preliminares. A ferramenta usada, ao permitir a simulação e execução passo a passo das tarefas, foi de grande valia para entendimento e aperfeiçoamento do modelo aqui proposto.

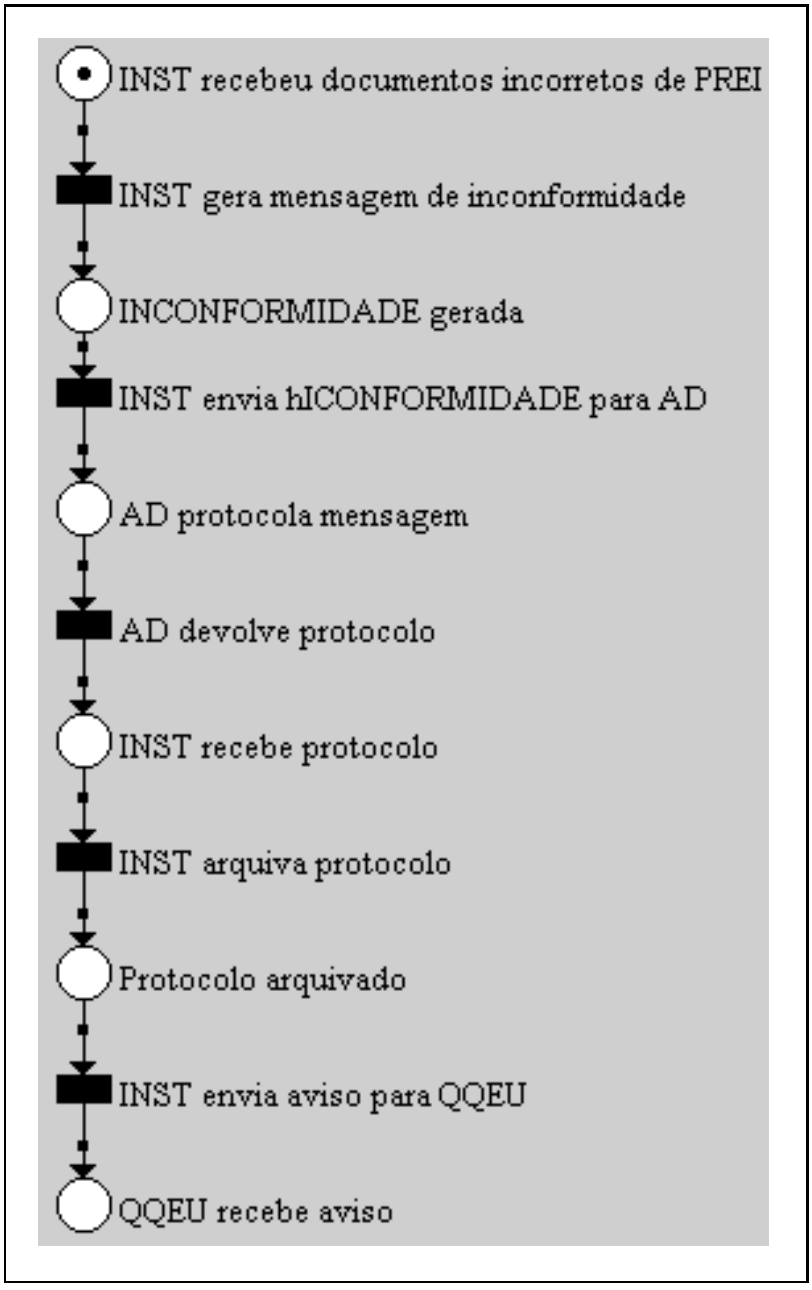

Figura 7.5: Inscrição não efetivada

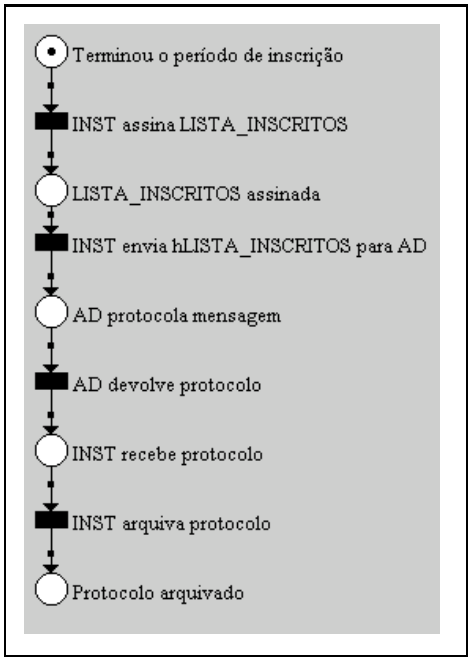

Figura 7.6: Terminou período inscrição

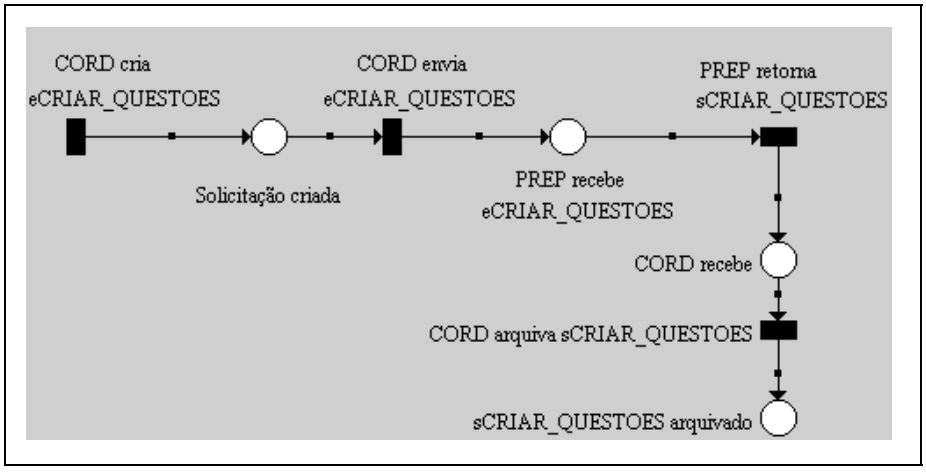

Figura 7.7: Coordenador solicita criação das questões

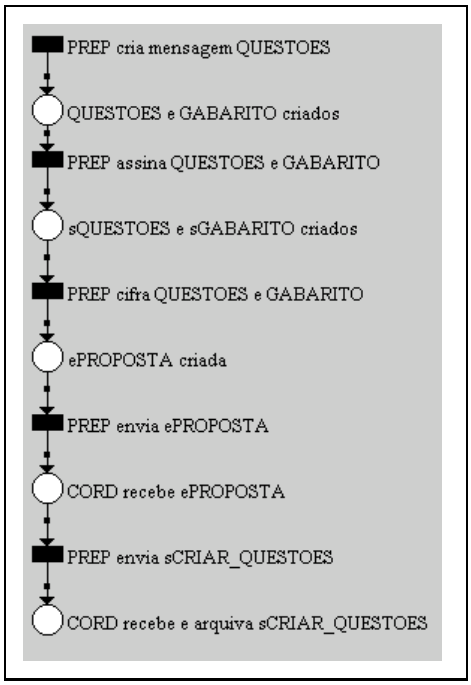

Figura 7.8: Preparador envia questões propostas

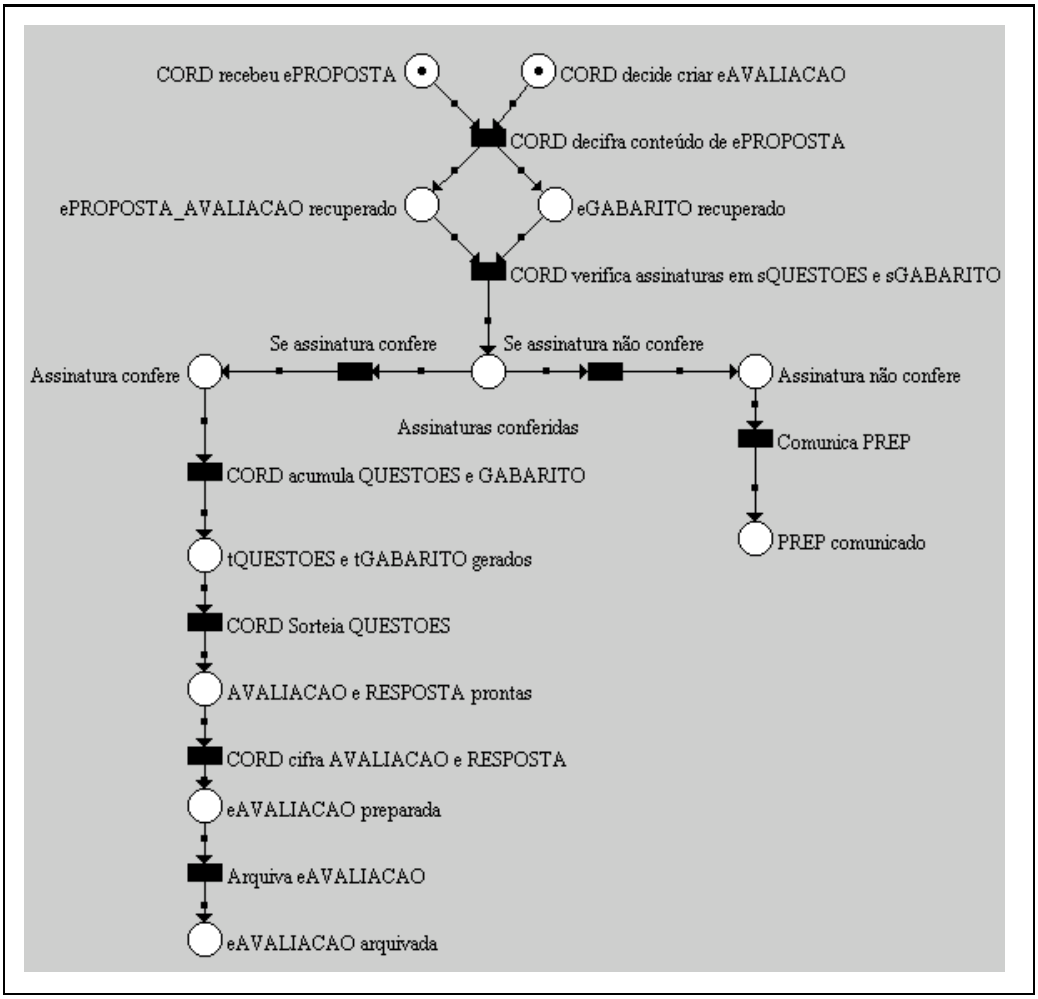

Figura 7.9: Coordenador cria avaliação

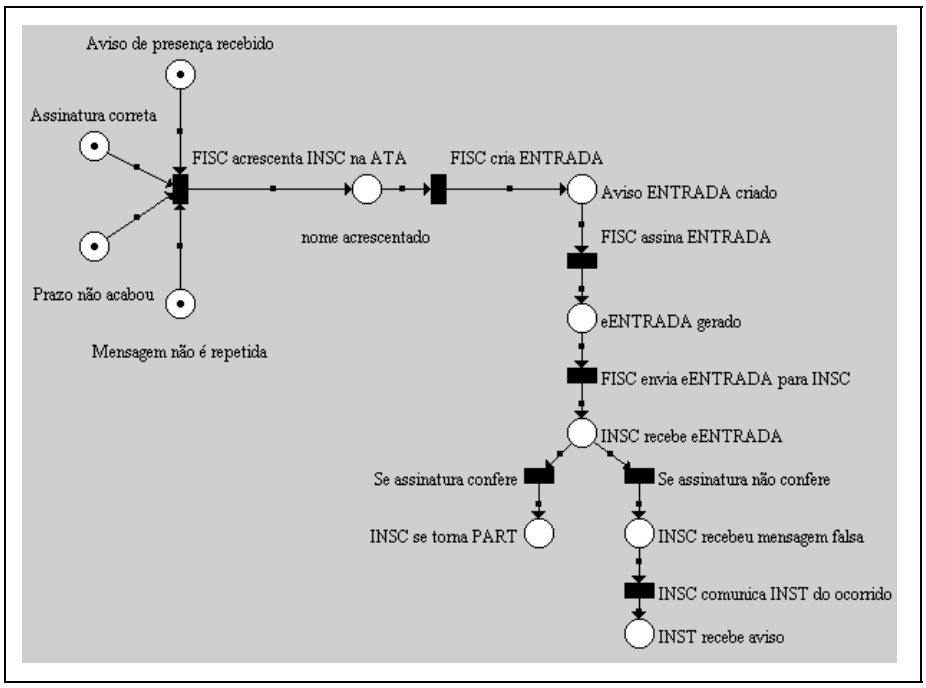

Figura 7.10: Inscrito avisa um fiscal que esta presente

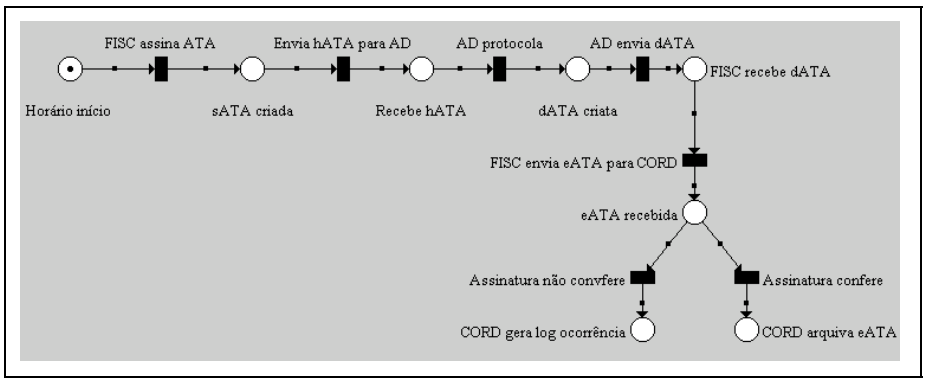

Figura 7.11: Fiscal entrega ata para o coordenador

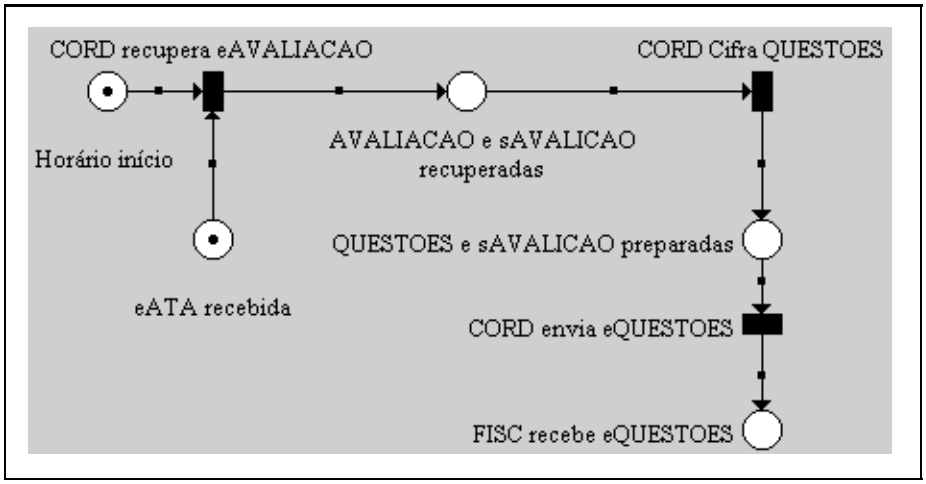

Figura 7.12: Coordenador autoriza o início

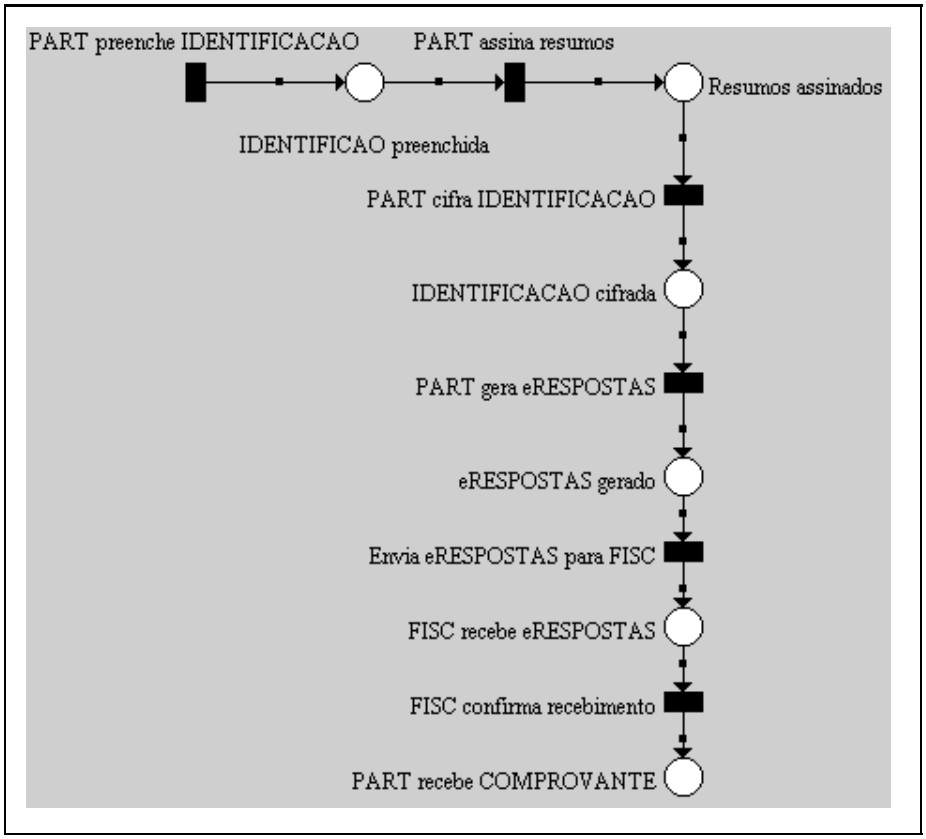

Figura 7.13: Participante envia respostas

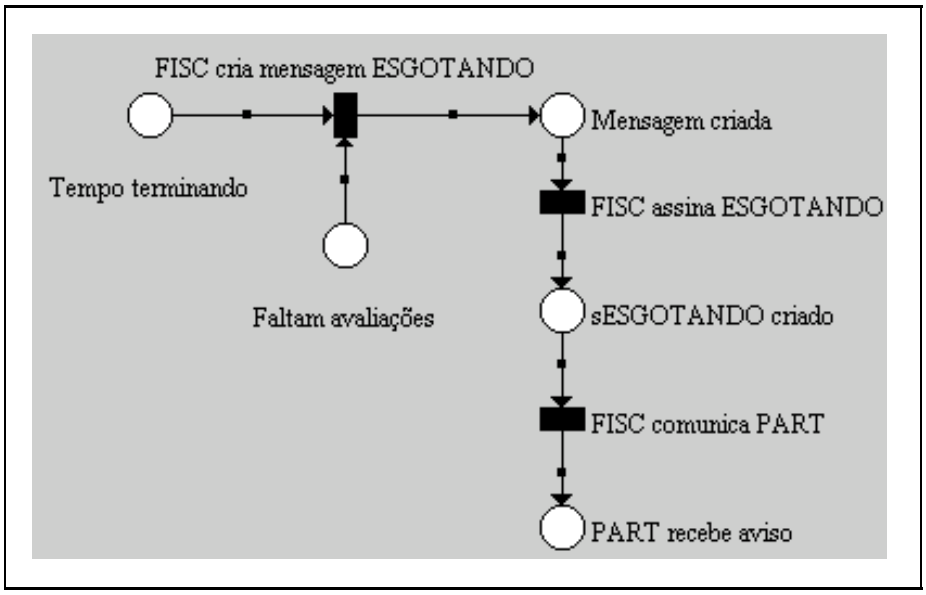

Figura 7.14: Fiscal avisa os participantes que o prazo de entrega das respostas esta terminando.

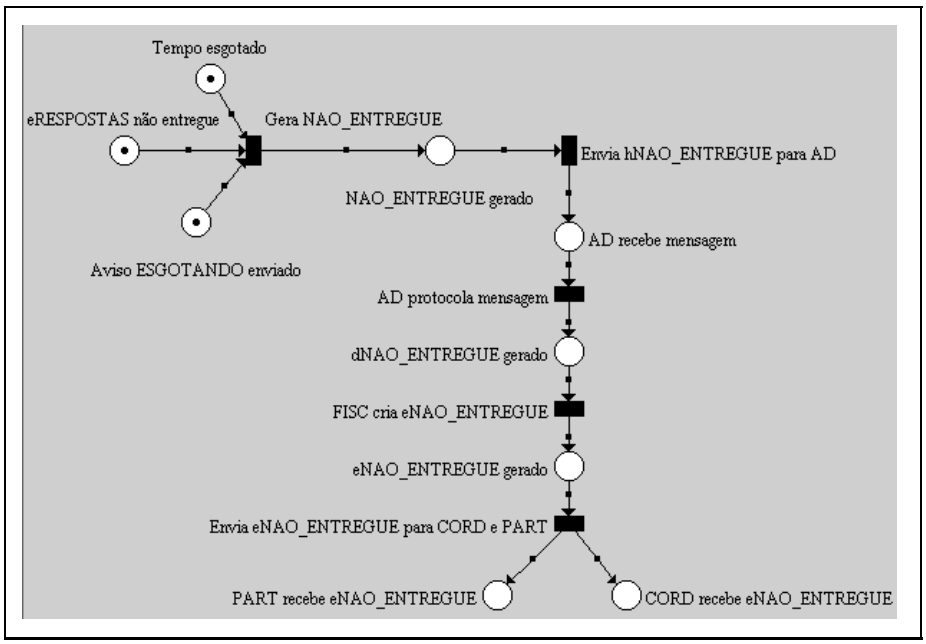

Figura 7.15: Fiscal registra com PDDE informação sobre as avaliações que não foram entregues.

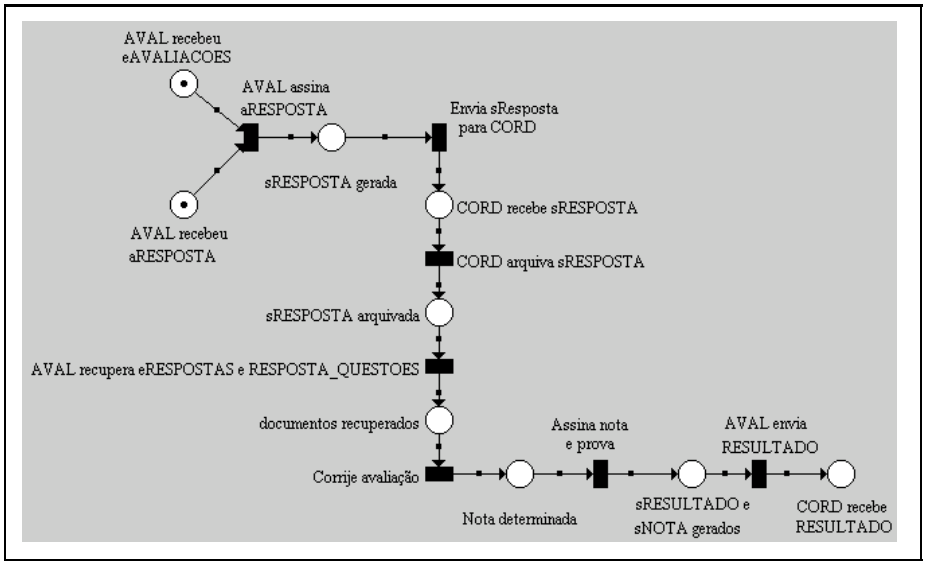

Figura 7.16: Apuração dos resultados.

Capítulo 8

Considerações Finais

Com o protocolo aqui proposto buscam-se novos meios para que a Internet possa ser usada como canal para realização de avaliações. O protocolo poderá poderá com certeza ser usado em sua totalidade para certificações profissionais. O uso em cursos a distância é limitado pela portaria número 2.253 de 18 de outubro de 2001 (DOU $19/10/2001$, p. 18, seção 1), que define o seguinte:

> "Os exames finais de todas as disciplinas oferecidas para integralização de cursos superiores serão sempre presenciais."

O que não gera impedimento do uso deste protocolo em avaliações diagnósticas. Em concursos e vestibulares a sua adoção poderá demorar mais. Contudo, o protocolo poderá ser usado em partes dos processos de concursos e vestibulares, tais como realização da convocação, inscrição, preparação e publicação. A aplicação da avaliação também poderá ser feita, se for empregado algum recurso de monitoramento dos avaliados. Para monitorar pode-se, por exemplo, usar o protocolo proposto por [FIO 00].

8.1 Alcance dos Objetivos

Inicialmente foi feito um estudo sobre as características dos diversos tipos de avaliação e o ensino a distância foi apresentado a seguir. Estes dois estudos possibilitaram o alcance dos primeiros objetivos específicos deste trabalho, listados abaixo:

- Determinar os principais locais onde avaliações são aplicadas;
- Definir atividades que fazem parte do processo de avaliação;
- Apresentar a importância das avaliações;
- Encontrar e descrever fases que compõem o processo de avaliação;
- Definir que documentos são necessários durante as fases que compõem o processo de avaliação;
- Verificar quando necessário as questões relacionadas com a legislação;
- Estabelecer as vulnerabilidades que poderiam advir da transformação do processo tradicional em um processo de avaliação não presencial a distância;

O estudo de técnicas criptográficas e a análise dos sistemas disponíveis possibilitaram uma visão geral sobre como o protocolo deveria ser estruturado do ponto de vista computacional, permitindo, desta forma, o alcance dos demais objetivos definidos para esta dissertação.

8.2 Contribuições

No conjunto que forma este trabalho, pode-se destacar dois grandes grupos. No primeiro tem-se um volume considerável de pesquisas voltadas para a área de ensino focando na atividade de avaliação. E no segundo se encontram os estudos feitos sobre segurança e a proposta de protocolo para *Segurança na Avaliação de Conhecimento em Contexto não Presencial* e sua respectiva formalização. Nestes grupos observa-se que foram feitas as contribuições a seguir:

- Revisão dos trabalhos existentes e dos conceitos pertinentes a avaliação do conhecimento. Esta revisão possibilitou o seguinte:
  - Determinar os principais locais onde avaliações são aplicadas;

  - Definir as atividades que fazem parte do processo de avaliação;
  - Definir que documentos são necessários durante o processo de avaliação;

- Inovação através do seguinte:
  - Base para unificação de diversos tipos de avaliações;
  - Criação de um protocolo que pode ser usado integral ou parcialmente na avaliação do conhecimento;
  - Criação de um protocolo que pode ser usado em todas as atividades de uma avaliação;
  - Validação do protocolo com Redes de Petri;

8.3 Trabalhos Futuros

A construção, implantação e uso do protocolo para *Segurança na Avaliação de Conhecimento em Contexto não Presencial* pode ser de grande valia para aperfeiçoar o protocolo aqui apresentado. Sugere-se ainda a implantação de alguma tecnologia que permita a monitoração dos avaliados durante a aplicação da avaliação. Mais estudos podem ser feitos para que, em vez da avaliação, gabarito e edital serem liberados pelo coordenador, sejam liberados para os interessados por alguma técnica de criptografia baseada em tempo (*time-released-cryptography*). Sugere-se ainda a definição de um processo de desenvolvimento que use a UML como ferramenta para projetar protocolos. Pode ser útil ainda a união desta proposta com o trabalho de [FIO 00]. Técnicas de criptografia de grupo podem vir a ser adotadas em substituição ao modelo aqui apresentado. De acordo com diversos autores, existem problemas relacionados com o desempenho neste tipo de criptografia.

Referências Bibliográficas

[ACA 02] ACADÊMICO, U. J. **O Resultado Na Internet**.

[AME 73] American, S., editor. **Cryptography and Computer Privacy**, 1973.

[AND 96] ANDERSON, R. Why criptosystems fail. **Practical Cryptography for Data Internetworks, IEEE Computer Society Press,**, [S.l.], v.I, 1996.

[AVA 98] AVANCINI, M. **Nove São Flagrados Com Cola Eletrônica**. Folha de São Paulo, Jan, 1998. 3-7 p. caderno COTIDIANO 1/5676.

[BER 98] BERGE, D. S. L. **Distance Training - How Innovative Organizations are**. Jossey-Bass, 1998.

[BL 98] BERNERS-LEE, T. **Uniform Resource Identifiers (URI): Generic Syntax**. Disponível em <http://www.ietf.org/rfc/rfc2396.txt. RFC diposnível em: http://www.ietf.org/rfc/rfc2396.txt.

[BOL 96] BOLIGNANO, D. An approach to the formal verification of cryptographic protocols. **IEEE**, [S.l.], v.I, 1996.

[CON 02] CONVEST. **Quadriênio 1998-2002**. Disponível em <http://www.convest.unicamp.br/vest2002/quadrienio/quadrienio.pdf. Relatório técnico sobre as atividades da comissão permanente de vestibular da UNICAMP.

[CUN 00] CUNHA, J. C. **Gerenciamento de Projetos de Ensino OnLine**. Universidade Datasul, 2000.

[DEV 01] DEVEGILI, A. J. **Farnel: Uma Proposta de Protocolo Criptográfico Para Votação Digital**. UNIVERSIDADE FEDERAL DE SANTA CATARINA, 2001. Dissertação de Mestrado.

[dINE 98] de Informática Na Educação, I. S. B., editor. **Investigando Educação a Distância e O Projeto Virtus Na UFPE**, Departamento de Informática Universidade Federal de Pernambuco - Cx. Postal 7851; 50.732-970; Recife-PE;Tel: (081) 271-8430, Fax (081)

271-8438;E-mail: ccrn,jngr,cagf@di.ufpe.br, 1998. Sociedade Brasileira de Computação (SBC).

[dMdM 97] de Medicina de Marília, F., editor. **Avaliação Do Estudante Na Aprendizagem Baseada Em Problemas**, Av. Monte Carmelo, 800, Marília SP, 1997. Faculdade de Medicina de Marília.

[dMFD 01] DE MATOS FERREIRA DINIZ, P. **Lei No. 8112 Regime Jurídico Único**. Brasilia Jurídica, 2001.

[DRI 98] DRISCOLL, M. **Web-Based Training**. 1. ed. San Francisco - Califórnia, 1998.

[dVLHMG 00] DE VIT ;LUCIANO HACK ;MARLISE GELLER, L. T. R. Supporting group learning and assessment through internet. **Biblioteca UFRGS http://www.pgie.ufrgs.br/webfolioead/biblioteca**, [S.l.], v.1, 2000.

[eC 01] E CULTURA, M. D. E. **Estatísticas**. http://www.mec.gov.br.

[ECO 99] ECO99, P. A. **Procurar Livro ECO99**. Procurar publicador ECO99, 1999.

[ESP 94] ESPARZA, J. On the decidability of model checking for several -calculi and petri nets. In: COLLOQUIUM ON TREES IN ALGEBRA AND PROGRAMMING, 1994. [s.n.], 1994. p.115–129.

[FIL 01] FILHO;, J. D. S. C. **Manual de Direito Administrativo**. Rio de Janeiro - RJ: Lumen Juris, 2001.

[FIO 00] FIORESE, M. Uma proposta de autenticação de usuários para ensino a distância. **SBRC 2000**, [S.l.], v.1, 2000.

[GHI 02] GHISLERI, A. S. A. **Sistema Seguro de Atendimento Ao Cliente - Garantia Da Qualidade de Serviço**. Universidade Federal de Santa Catarina, 2002. Dissertação de Mestrado.

[GIU 00] GIULI, D. The learning tutor: A web based authoring system to support distance tutoring. **Journal of International Forum of Educational Technology and Society And IEEE Learning Technology Task Force**, [S.l.], v.3, 2000.

[ISE 00] ISENHOUR, P. L. The virtual school: An integrated collaborative environment for the classrrom. **Journal of International Forum of Educational Technology and Society And IEEE Learning Technology Task Force**, [S.l.], v.3, 2000.

[JAC 94] JACOBSON, R. L. Computerized testing runs into trouble: Political and technical questions are raised. **The Chronicle of Higher Education**, [S.l.], v.1, p.A16–A17, 1994.

[JAC 95] JACOBSON, I. J. E. **The Object Advantage - Business Process Reengineeering with Object Technology**. ACM European Service Center - Avenue Marcel Thiry 204 1200 Brussels, Belgium Phone 32-2-774-9602: Addison Wesley, 1995.

[JAC 98] JACOBSON, G. B. R. I. **The Unified Software Pocess**. One Jacob Way - Massachusetts 01867: Addison Wesley, 1998.

[JC 97] JANETTE CARDOSO, R. V. **Redes de Petri**. Editora da UFSC, 1997.

[JOH 91] JOHANSEN, R. **Leading Business Teams : How Teams Can Use Technology and Group Process Tools to Enhance Performance**. Addison-Wesley Series on Organization Development. Nova Iorque;EUA: Addison-Wesley, 1991. 13-37 p.

[LAU 01] LAUGNA;, R. L. D. S. J. I. W. D. H. F. A. **Comércio Eletrônico**. SP: Instituto dos Advogados de São Paulo e Editora Revista dos Tribunais, 2001.

[MAD 71] MADAUS, B. S. B. T. H. G. **Handbook on Formative and Summative Evaluation of Student Learning.** New York: McGraw Hill Co; New York, 1971.

[MAL 00] MALER, T. B. P. M. S.-M. **Extensible Markup Language (XML) 1.0 (Second Edition) - W3C Recommendation 6 October 2000**. Disponível em <http://www.w3.org/TR/2000/REC-xml-20001006. This document specifies a syntax created by subsetting an existing, widely used international text processing standard (Standard Generalized Markup Language, ISO 8879:1986(E) as amended and corrected) for use on the World Wide Web. It is a product of the W3C XML Activity, details of which can be found at http://www.w3.org/XML. The English version of this specification is the only normative version. However, for translations of this document, see http://www.w3.org/XML/trans. A list of current W3C Recommendations and other technical documents can be found at http://www.w3.org/TR.

[MEN 96] MENEZES, A. **Handbook of Applied Cryptography**. CRC-Press, 1996.

[NEW 97] NEWTON, D. E. **Encyclopedia of Cryptology**. Santa Barbara: ABC-CLIO, Inc., 1997.

[OLI 00] OLIVER, M. An introduction to the evaluation of learning technology. **Journal of International Forum of Educational Technology and Society And IEEE Learning Technology Task Force**, [S.l.], v.3, 2000.

[PAS 02] PASQUAL, E. S. **Uma Infra-Estrutura Para a Datação de Documentos Eletrônicos**. UFSC - Universidade Federal de Santa Catarina, 2002. Dissertação de Mestrado.

[PJ 01] PAGE-JONES, M. **Fundamentos Do Desenho Orientado a Objeto Com UML**. Rua Tabapuã 1348, Itaim-Bibi - CEP 04533-004 - São Paulo - SP: Makron Books, 2001.

[QUA 98] QUATRANI, T. **Visula Modeling with Rational Rose and UML**. Addison Wesley, 1998.

[ROG 95] ROGAWAY, M. B. Provably secure session key distribution. **ACM Symp. on Theory of Computing**, [S.l.], v.I, 1995.

[SCH 98] SCHNEIER, B. **Applied Cryptography - Protocols Algoritms and Source Code in**. Wiley, 1998.

[SCH 01] SCHNEIDER, P. R. . S. **Modelling and Analysis of Security Protocols**. London - Great Britain: Addison Wesley, 2001.

[SHE 96] SHERRY, L. Issues in distance learning. **International Journal of Educational Telecommunications**, [S.l.], v.1, p.337–365, 1996.

[SPO 96] SPODICK, E. F. **The Evolution of Distance Learning**. http://sqzm14.ust.hk/distance/evolution-distance-learning.htm.

[STA 99] STALLINGS, W. **Cryptography and Network Security: Principles and Practice**. Prentice Hall, 1999.

[STI 95] STINSON, D. **Cryptography: Theory and Practice (Discrete Mathematics and Its Applications)**. CRC Press, 1995.

[tACSAC 95] 11th Annual Computer Security Application Conference, editor. **Role-Based Access Control - RBAC: Features and Motivations**, New Orleans, LA, 1995.

[TAR 00] TAROUCO, L. **O Processo de Avaliação Na Avaliação a Distância**. Biblioteca virtual da Universidade Federal do Rio Grande do Sul. http://www.pgie.ufrgs.br/webfolioead/biblioteca/biblioteca.html.

[UDE 01] UDESC. **Vestibular Vocacionado 2002/01 - Inscrição Via Internet**.

[VAS 98] VASCONCELLOS, C. D. S. **Avaliação Da Aprendizagem: Práticas de Mudança**, v.6 of **Cadernos Pedagógicos Do Liberdad**. 1998.

[WIN 98] WINTERS, G. S. P. **Applying Use Cases - A Practical Guide**. Addison-Wesley, 1998.

[YOU 96] YOUMAN, R. S. E. C. H. F. Role-based access control mode. **IEEE Computer**, [S.l.], 1996.

Apêndice A

Glossário

avaliar - Determinar a valia ou o valor de.

avaliação - Ato ou efeito de avaliar.

avaliador - Que ou aquele que avalia.

cifrar - Escrever em cifra, ou seja, criptografar um texto aberto.

criptografar - Tornar incompreensível, com observância de normas especiais consignadas numa cifra ou num código, o texto de (uma mensagem escrita com clareza).Codificar (uma informação) de forma a tornar difícil sua decodificação sem a chave (20) adequada.

criptografia - Arte de escrever em cifra ou em código. Conjunto de técnicas que permitem criptografar informações (como mensagens escritas, dados armazenados ou transmitidos por computador, etc.).

web - De Worldwide Web, recurso ou serviço oferecido na Internet (rede mundial de computadores), e que consiste num sistema distribuído de acesso a informações, as quais são apresentadas na forma de hipertexto, com elos entre documentos e outros objetos (menus, índices), localizados em pontos diversos da Rede. 2. O conjunto das informações e recursos assim disponibilizados.

internet - Qualquer conjunto de redes de computadores ligadas entre si por roteadores e gateways, como, por exempo, aquela de âmbito mundial, descentralizada e de acesso público, cujos principais serviços oferecidos são o correio eletrônico, o chat e a Web, e que é constituída por um conjunto de redes de computadores interconectadas por roteadores que utilizam o protocolo de transmisso TCP/IP.

log - Arquivo de registro automático de operações efetuadas num computador.

navegador - Aplicativo, ou parte de aplicativo, capaz de apresentar o conteúdo de um sistema de hipertexto ou de hipermídia e permitir a navegação neste; browser, leitor de hipertexto.

site - Qualquer servidor da Web, ou, por extensão, o endereço (v. URL) em que este pode ser acessado. Podendo ainda ser interpretado como o conjunto de documentos apresentados ou disponibilizados na Web por um indivíduo, instituição, empresa, etc., e que pode ser fisicamente acessado por um computador e em endereço específico da rede.

software - Em um sistema computacional, o conjunto dos componentes que não fazem parte do equipamento físico propriamente dito e que incluem as instruções e programas (e os dados a eles associados) empregados durante a utilização do sistema. Qualquer programa ou conjunto de programas de computador: um software para processamento de texto.

URL - Sigla do ingls u(niform) (ou, originalmente, universal) r(esource) l(ocator), 'localizador uniforme (ou universal) de recursos'. Serve para designar a localização de um objeto na internet (rede mundial de computadores), segundo determinado padrão de atribuição de endereços em redes.

vestibular - Exame de admissão a qualquer escola de nível superior.

WWW - Sigla do inglês W(orld) W(ide) W(eb), veja também web.